2B Advice

The Privacy Benchmark

Data Protection Practice in Businesses 2015

In Cooperation With:

EU Data Protection

Data Protection
in the European Union

IWuS

Technical University
of Dortmund

Data Protection Practice in Businesses 2015

Legal Information

2B Advice GmbH

Represented by the Managing Directors:
Marcus Belke and Hans Joachim Bickenbach

Joseph-Schumpeter-Allee 25
53227 Bonn
Germany

Phone: +49 228 926165-100
Fax: +49 228 926165-109
E-Mail: info@2b-advice.com

Commercial Register Number: Bonn HRB 12713

Contributors

Björn Malinka (Consultant – 2B Advice GmbH)
Erin Donaldson (Marketing Web & Graphics – 2B Advice LLC)
Karsten Neumann (Associate Partner – 2B Advice GmbH)
Amelie Sophia Schleip (Student – 2B Advice GmbH)
Sophie Tchanyou Ganme (Student – TU Dortmund)
Dr. Dominik Wied (Junior Professor, Business and Social Statistics – TU Dortmund)
Dominik Zier (Consultant – 2B Advice GmbH)

Table of Contents

Dear Reader,

The new General Data Protection Regulation is being widely discussed. What role this will assign to data protection officers in Europe, however, is not yet certain. At present, it seems rather unlikely that the institution of the data protection officer will be introduced as mandatory in all European countries. Public discourse about the role of the data protection officer is, meanwhile, characterized by understatement, exaggeration, poor technical knowledge and fear. Some see the data protection officer as a "bureaucratic monster hostile to innovation." Others regard it as a heroic spearhead in the struggle against states and organizations that collect data unscrupulously. Both of these viewpoints are far from reality. "Data Protection Practice 2015," a study conducted by the 2B Advice business consultancy, seeks to make the discussion more objective. For the second time since 2012, we have conducted an empirical study of everyday data protection practices in German companies and presented the results. In the study, data protection officers talk about their everyday practice, anonymously and away from the headlines. They provide information and suggestions on how a socially acceptable balance can be struck between commercial interests and the protection of citizens' privacy. At the same time, data protection officers call for action in politics and business. According to the findings, 77% of data protection officers in Germany expect the level of data protection in the country to fall as a result of the General Data Protection Regulation. Meanwhile, 79% state that they receive "satisfactory" or "fairly satisfactory" support from their management, which represents a significant improvement on the findings in 2012. 69% believe the existing data protection legislation, particularly concerning social media, cloud computing and international data processing, to be unfeasible.

It surprised me to learn that almost half the data protection officers in the study (44%) are dissatisfied with the regulatory authorities. Here the data protection officers would like to see more inspections, more advice and more training. Other surprising outcomes: Only 37% of the data protection breaches detected affected customers, while 48% affected the company's own employees. Here internal monitoring within companies should be intensified.

The typical data protection officer (81% of those questioned) works part-time. 37% are able to devote a maximum of just 5% of their work time to data protection. They work with high efficiency, however, when it comes to measures such as sensitizing employees to data protection issues, communicating with the regulatory authorities and advising company departments in the planning phases of projects.

This study gives realistic insight into the work of data protection officers, the resources they use and approaches to improvements which are being put into practice. Overall, it makes a case for the introduction of data protection officers throughout Europe.

Sincerely,
Marcus Belke

Attorney
Managing Director, 2B Advice GmbH

Photo credit: © Axel Voss

Data protection has never been more relevant than it is today. Like no other technical revolution before it, digitalization is changing our social and professional behavior, our communication, our competitiveness, national relations, criminal prosecution, individual and property rights, copyright and intellectual property – right down to our basic right to data protection and, more fundamentally, our right to personal privacy. Practically all areas of our lives involve data. Data is the currency of the future!

The challenges that come with technological development, the Internet, and globalization have neither been realized nor governmentally regulated to the full extent necessary. Those who wish to regulate how data is handled are confronted with questions on the preservation of fundamental rights, global competition and growth, and matters of security.

Organizational structures are becoming less and less transparent, and data breach scandals are shaking consumers' confidence. This decline in confidence is demonstrated by the present study, which also provides both policymakers and those in industry with concrete numbers about the work of data protection officers in Germany. The long-term goal is a domestic European digital market with high standards for data protection. Negotiations for the EU General Data Protection Regulation are proceeding into their final phase. That is why we need to take into account waning consumer confidence, as well as the concerns of German data protection officers, for the coming revisions to the EU regulation. Most importantly, we must adapt European data protection to the digital world, a process in which data protection officers will play an important role.

Sincerely,
Axel Voss

Member of the European Parliament
Deputy Chairman of the Committee on Legal Affairs
Legal Policy Spokesman of the CDU/CSU Group

1. Introduction

Photo credit: © twobee - Fotolia.com

With its report "Data Protection Practice 2012," international data protection consultancy 2B Advice - the privacy benchmark presented the first study in the field about the practices of data protection officers in German companies. Detailed answers by almost 400 company data protection officers were collated for the first time to produce a more accurate picture of the degree of practical implementation of German data protection guidelines, which has subsequently influenced discussions in Europe about the drafting of a general European data protection regulation. The vice president of the European Commission at the time, Viviane Reding, emphasized that the study was received by the European Parliament in Brussels in November 2012 in time to influence the advisory process on a unified European data protection concept.

By analyzing the practical experience of data protection officers in the business sector, the study confirmed efficacy of this model of corporate self-monitoring, but it also identified an urgent need for action to be taken by both companies and legislators. MEP Axel Voss stressed in particular the effectiveness of in-house data protection officers based on empirical data: "On-site, built-in data protection in the company itself has proven to be a successful model in Germany. We want to turn this into a major export success for the rest of Europe," read his statement during the presentation.

2B Advice, again in cooperation with the Technical University of Dortmund, now presents "Data Protection Practice 2015." By repeating our examination in 2014, we were able to reexamine our empirical data from 2012. By fine-tuning questions from the previous study, we have eliminated possible errors and misunderstandings for the current study. At the same time, two more years of development trends in the history of data protection have been captured – trends characterized by intensive professional and political discussion.

Once again we interviewed data protection officers across Germany in companies ranging from international corporations to small- and medium-sized businesses, some with many years of experience. 62% of respondents had taken part in the 2012 study while 38% were taking part for the first time. The gaps in representation among the participating industries and company sizes are the logical consequence of the participant group since only companies with an appointed data protection officer were included in the study. A total of 2,097 years of data protection experience has been taken into account in this study (see section 4.9.3).

The discussion in Europe has left a noticeable mark in the "Data Protection Practice 2015" study: 23% of the data protection officers questioned expect an improvement in the level of data protection in Germany, while 77% of those questioned anticipate it to worsen. The level of expectation has dropped significantly here. In 2012, 41% of data protection officers expected an improvement in the level of data protection; in 2014, the skeptics are even more pronounced (see 4.10.5).

2. Overview of Main Findings

The study reflected all aspects of in-company data protection in German companies in concentrated form. Factors including the implementation of the obligation to employ a data protection officer, the organization of data protection management processes, experiences with regulatory authorities and data protection breaches and sanctions were covered, together with assessments of the need for legislative action in Germany and Europe.

Structure of the Companies Surveyed

Across Germany, 15% of the participating companies employ up to 50 employees, 45% up to 500, 30% up to 5,000, 9% up to 50,000 and 1% over 50,000. It can be seen that data protection officers from large companies made up a disproportionately large number of the participants. This can be attributed to the data collecting methodology. The survey was addressed to data protection officers known by name, which is why companies without a data protection officer were left out.

In-Company Data Protection Practice

In 34% of the companies, a data protection officer has been employed only in the last five years. The average data protection officer generally works alone with too little time and insufficient resources. The legal prerequisite governing the legitimacy of the appointment of a data protection officer is his or her suitability for fulfilling his or her duties. This includes the granting of sufficient work time. With the decision of the Düsseldorfer Kreis from November 24-25, 2010, the highest regulatory authorities in Germany formulated the minimum requirements for the expertise and independence of data protection officers under section 4f para. 2 and 3 of the Federal Data Protection Act (BDSG) but did not specify the time requirement in more detail.

> *"48% of the data protection officers questioned do not have enough time to fulfill their statutory obligations."*

The utilization and workload of data protection officers is principally influenced by the size of the relevant company, the number of companies for which the data protection officer is responsible, the particularities of data processing in the particular industry and the level of protection required for the processed personal data. According to the outcomes of the study, 81% of data protection officers work part-time and 19% full-time. This proportion has not changed since 2012. The part-time group has therefore been questioned in greater detail in the 2015 study. Of those questioned, 37% of data protection officers are able to devote a maximum of 5% of their work time to data protection. Just over half of the data protection officers questioned (52%) consider the time available to them to be satisfactory. From this, it can be concluded that 48% of the data protection officers questioned believe that their appointment does not satisfy the requirements of the Data Protection Act. If insufficient time is available, a data protection officer is regarded as not effectively appointed. Apart from the restricted effectiveness of the work itself, this also means a heightened risk of fines being imposed (see 4.2.4).

In-Company Data Protection Breaches

Only 58% of the data protection officers questioned feel adequately informed about possible data protection breaches within their company (see 4.3.1). Section 42a of the Federal Data Protection Act (BDSG, Bundesdatenschutzgesetz) postulates an obligation to notify the responsible person or office in the event of unlawful acquisition of personal data by a third party if this threatens serious harm to the rights or legitimate interests of those affected. This relatively new regulation in the BDSG has caused much uncertainty and need for clarification within the profession. The results of the survey give clear proof of the relevance of such assessments since 28% of the data protection officers questioned have already had to make such an assessment (see 4.3.3). The growing relevance of this can be seen from a comparison with the results of the "Data Protection Practice 2012." Then only 21% of data protection officers stated that they had already had to make an assessment of this kind.

> *"42% of the data protection officers questioned were not satisfactorily informed of data protection breaches."*

In those cases in which detected data protection breaches were punished, the data protection officers questioned responded at a rate of 74% that they were "hardly" or "not at all" satisfied with the subsequent corrective action (see 4.3.13). Such dissatisfaction can perhaps be explained by insufficient consequences (47% stated that these consisted solely of rectifying the fault [see 4.3.12]). This result is surprising when compared with the results of the 2012 survey. At that time, the majority (63%) of the data protection officers responded that they were "fairly" or "very" satisfied with the corrective action.

The In-Company Data Protection Officer

Nevertheless, 21% of the data protection officers questioned rated the level of support they received from management as "unsatisfactory" or "fairly unsatisfactory," while 79% rated their support as "satisfactory" or "fairly satisfactory" (see 4.4.6). However, an improvement can still be seen here compared to the responses to this question in "Data Protection Practice 2012." At that time, 33% evaluated support by management as unsatisfactory. Again this shows an existing discrepancy between the legislative intention and the reality in business practice.

The Privacy Inventory Tool

8% of the data protection officers questioned and already appointed stated that their company still did not have a privacy inventory tool (see 4.5.1). In particular, the data controller, the group of data subjects affected, the type of data, the intended purpose and the data security precautions are to be documented in the overview of all automated processes. When asked about the number of individual procedures within one processing overview, the data protection officers questioned reported an average of 57 procedures (see 4.5.2).

Naturally, this number varies considerably with the size of the company. Thus, 46% of the companies with up to 50,000 employees stated that their privacy inventory tool covered up to 500 individual procedures. In companies with fewer than 5,000 employees, this figure is still 10%. These figures make it clear that maintaining the inventory is a substantial piece of work in organizational terms that requires significant resources. In the group of companies with under 50 employees, by contrast, more than 90% of privacy inventory tools contain no more than 50 different procedures.

"62% of the data protection officers questioned do not have a complete privacy inventory tool."

Only 38% of the data protection officers questioned answered that all the procedures of their company were recorded in the privacy inventory tool (see 4.5.3). However, since this overview of all automated procedures must be complete, the absence of a procedure in the privacy inventory tool constitutes a breach of the company's obligations under section 4g para. 2 of the BDSG. The respondents who replied that their privacy inventory tool was incomplete were then asked to specify the percentage of completion of the privacy inventory tool in order to gain a clearer understanding. On average, a degree of completeness of about 60% was reported (see 4.5.3.2).

"13% of the data protection officers questioned do not inspect contract data processors."

Under section 11 of the BDSG, the client remains legally responsible for data protection when it commissions a third party to process personal data. It has extensive inspection obligations which, however, it may exercise at its discretion. No specific form of monitoring is legally prescribed. Self-inspection (35%) and the number of certifications obtained (31% of all responses), the latter figure 10% greater than in 2012, are among the inspection procedures stated most frequently (see 4.5.10). Despite the fact that the situation is clearly unlawful, 13% of respondents stated that no inspections were carried out. Only in a few cases were on-site audits carried out, either by service providers paid by the company or by independent third parties paid by the contractor.

Certification

Only 5% of the data protection officers questioned stated that their company had already obtained a data protection certification (see 4.6.1). However, 43% of the data protection officers questioned regarded certification as useful.

"43% of the data protection officers questioned regard certification as useful."

According to the data protection professionals questioned, no data protection certification had been obtained in their companies, primarily because the costs were too high (28% of all responses). Other reasons given were unclear acceptance by the regulatory authorities (19%), internal costs which would be too high (19%) and costs of an external audit which would be too high (16%). The least frequent responses were lack of international acceptance (13%) and the risk of failing the audit (6%) (see 4.6.3).

Regulatory Authorities

Enthusiasm among data protection officers for inspections by the regulatory authorities is still limited; nevertheless, 46% of respondents would like more inspections (see 4.7.1). In almost complete agreement with this, the data protection officers demand more consultancy activity on the part of the regulatory authorities (92%) and for them to offer training (76%). Similarly, the majority (62%) of the data protection officers also demanded certification through the regulatory authorities.

"44% of the data protection officers questioned are dissatisfied with the work of the regulatory authorities."

44% of the data protection officers questioned considered the actions of the regulatory authorities to be too inconsequential (see 4.7.2). Thus, a proportion of the respondents (11% greater than in 2012) regard the regulatory authorities as something of a "toothless tiger." This tendency should be a cause for concern for the regulatory authorities.

In the experience of 53% of the data protection officers, data protection breaches are not satisfactorily prosecuted by the regulatory authorities (see 4.7.3). Compared to the result in "Data Protection Practice 2012," this opinion has increased by 5%.

To summarize, it can be said that the prosecution of data protection breaches by the regulatory authorities was rated by almost half the data protection officers as unsatisfactory and therefore as inconsequential.

Legal Issues

The data protection professionals expressed almost unanimous need for action at the legislative level. A large majority of the data protection officers questioned, an increase by 6% compared to the 2012 results, wish primarily to see changes in the law relating to online data protection (79%), personal Internet and e-mail use at work (77%) and data protection for employees (72%). The data protection officers also see the need for action on the regulations on transborder data flows (69%) and on contract data processing (59%) (see 4.8.2).

"Data protection officers are calling for protection against domestic and foreign surveillance."

The participants had the opportunity of stating additional topics requiring legislative action in a free-text field. As well as the topics covered in the study, the total of 44 suggestions included repeated demands for a clarification of the powers of the police and public prosecutor's department to act against criminal activity by companies and for resolution of the contradictions between data protection for employees and customers on one hand, and the compliance requirements of terrorism blacklists, authorized economic operator (AEO) certification and similar statutory requirements on the other. Protection against domestic and foreign state surveillance was also identified here as an area in which legislation should be updated (see 4.8.4).

Training for Data Protection Officers

The BDSG sets out personal and technical requirements for the appointment of a data protection officer; these have been made concrete by a decision of the supreme regulatory authority. There exists no vocational training or professional qualification to date grounded in legislation. This deficiency is an issue of complaint not only for trainers and the professional association; 67% of respondents to the survey also argue for legally regulated training (see 4.9.1). This confirms the result from 2012 (64%).

50% of the participating data protection officers stated that they obtained their qualifications by means of continuing professional training measures; 28% rely on experience gained in the course of their work and 15% rely on prior knowledge obtained from a course of study (see 4.9.2). These results demonstrate that the required qualifications are generally gained through continuing professional development (CPD) and experience gained on the job.

EU General Data Protection Regulation

The European legislative debate in the past three years has left its mark; 23% of the data protection officers questioned expect an improvement in the level of data protection in Germany, while 77% of those questioned anticipate it to worsen. The level of expectation has dropped significantly here (see 4.10.5). In 2012, 41% of the data protection officers questioned expected an improvement in the level of data protection, while in 2014 there are noticeably more skeptics.

"77% of the data privacy officers questioned expected a deterioration in the level of data protection in Germany through the EU GDPR."

3. Methodology and Operational Procedure

Once again we have been supported by the Department of Business and Social Statistics at the Technical University of Dortmund, headed by Prof. Dr. Walter Krämer, in devising, performing and evaluating this study. As with the 2012 study, published contact information of data protection officers in German businesses was used to invite the respondents to participate. The participants in the 2012 study were drawn from the same source.

62% of respondents had taken part in the 2012 study, while 38% were taking part for the first time. The gaps in representation among the participating industries and company sizes are the logical consequence of the participant group since only companies with an appointed data protection officer were included in the study.

Data protection officers who had agreed to the use of their e-mail address for marketing purposes were invited to participate in the survey by e-mail, with a link to a special online instance of the questionnaire prepared for that individual; this instance was then anonymized immediately upon successful completion. Those participants who received postal invitations were sent a login ID that they could use in conjunction with their e-mail address to participate. Both groups also had the option of printing the questionnaire and sending it in. Each e-mail address was allowed to participate only once. This enabled external data protection officers to take part on behalf of multiple companies by using a different e-mail address for each, for example, and requesting more than one ID. Such external data protection officers, thus, had the possibility of indicating differing conditions in the various companies.

The companies with under 50 employees are considerably under-represented in comparison to the company structure in our survey. This is unsurprising since these companies often do not publish the names of their data protection officers and, thus, could not be included in the distribution list for this survey.

The companies with between 50 and 500 employees are over-represented for the opposite reasons. Here the information is far more frequently made public. Moreover, above a certain company size, data protection officers tend to be more interested in cooperation. Instead of the statistical fraction of about 20%, they appear in the survey roughly twice as frequently at a rate of 45%.

Companies with over 500 employees formed the second largest group within the study participants: while they only represent about 2% of companies in Germany in general, they make up exactly 40% in terms of the number of participating data protection officers.

In summary, it may be said that the results substantially reflect the opinions and assessments of data protection officers from relatively large companies: 40% of respondents came from companies with over 500 employees, and a further 10% were from companies with over 5,000 employees.

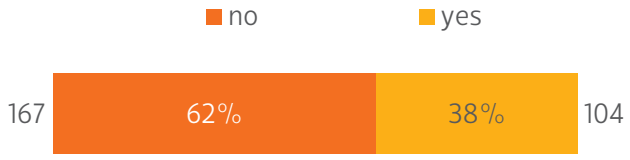
This is underpinned by certain other results, e.g. information on the international nature of the companies and information on the frequency of audits by the regulatory authorities.

For this survey, however, it was not the representativity of the participating companies in relation to the statistical average size of German companies that was the determining factor, but rather a clear picture of data protection practices in those companies that have already appointed a data protection officer. “Data Protection Practice 2015” therefore emphasizes a qualitative evaluation of the implementation of the requirements of data protection legislation in German companies.

Deviations in the totals arise because not every respondent answered every question in the questionnaire.

4. The Results in Full

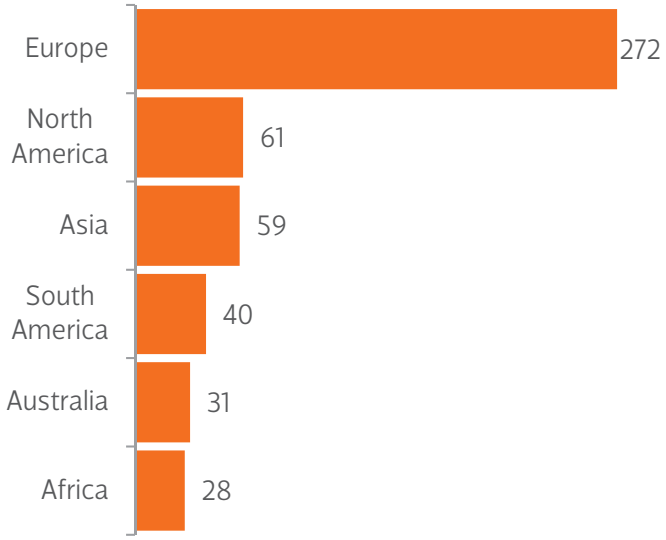
Did you take part in the 2012 study?



Only 38% of the data protection officers questioned had previously participated in "Data Protection Practice 2012" survey. This is of interest for purposes of observing and interpreting individual topics and questions. Since most of the questions from 2012 were adopted unchanged for the 2015 study, it was possible to directly observe changes in opinion since 2012 while also including the perspectives of additional data protection officers not previously questioned. Furthermore, it was possible to clarify or extend other questions that had previously been subject to misunderstandings in order to corroborate and/or correct the results of "Data Protection Practice 2012." Consequently, a consolidated representation was obtained from the 2012 and 2015 outcomes together with valid statements about the work of data protection officers in Germany.

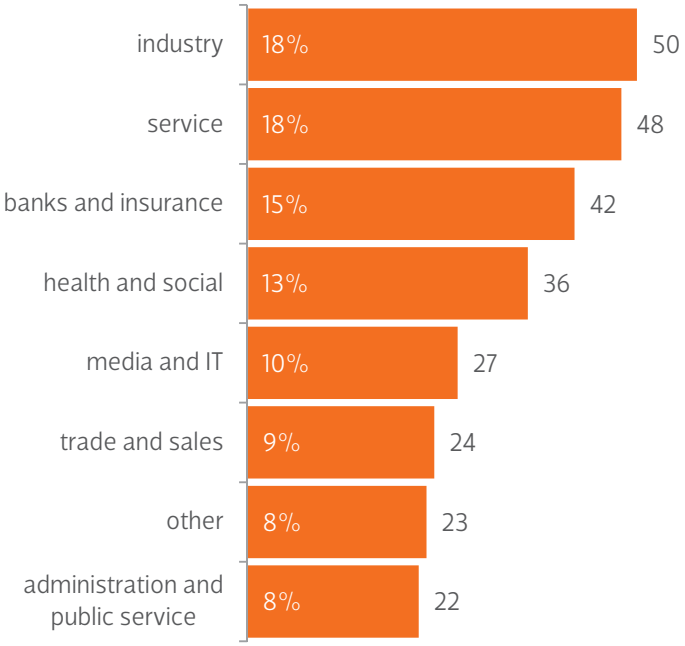
4.1 Structure of the Companies Surveyed

1. On which continents is your company represented?



Of the 272 participating companies, 59 are also represented in Asia, 28 also in Africa, 31 also in Australia, 61 also in North America and 40 also in South America by an office. Thus, the professional expertise of both small and medium-sized companies and also internationally active German corporations are reflected in the outcomes of the study. Small and medium-sized businesses are also increasingly internationally active and are having to face the specific challenges of international data flows.

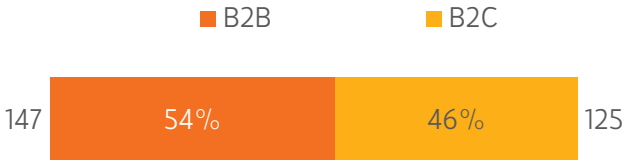
2. In which industry does your business primarily operate?



Of the 272 data protection officers, 50 (18%) stated that their business operated primarily in industry, a further 48 (18%) in the services sector, 42 (15%) in insurance, 36 (13%) in the health and social sector, 27 (10%) in media and IT, 24 (9%) in trade and marketing, 22 (8%) in administration and public services and finally 23 (8%) in other sectors than the above.

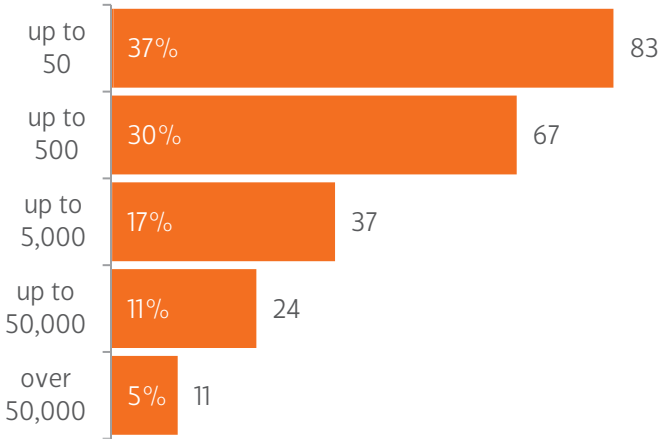
These figures verify that the requirement of the study to represent the work of data protections officers from the entire spectrum of German companies was met.

3. What is the primary nature of the business relationships in your company?



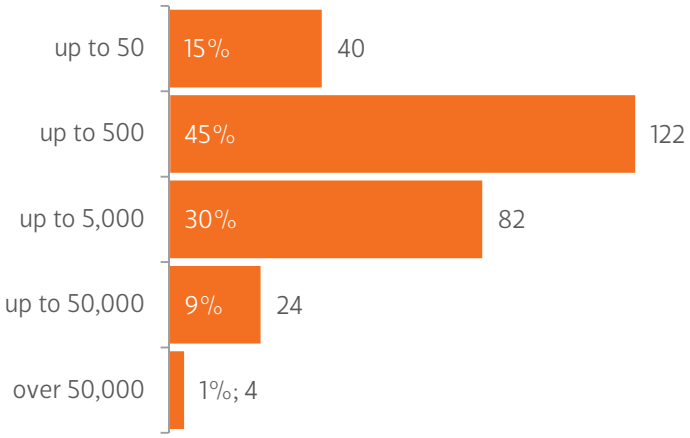
A little over half of the data protection officers (54%) stated that most of the business relationships in their companies were business-to-business (B2B) relationships. Accordingly, the areas of data processing relevant for data protection law are portrayed almost equally.

4. How many employees does your company employ worldwide, not including Germany?



Of a total of 222 participants who answered this question, 37% stated that they worked as data protection officers in companies with up to 50 employees, 30% in companies with up to 500 employees, 17% in companies with up to 5,000 employees, 11% in companies with up to 50,000 employees and 5% in companies with over 50,000 employees. It can be seen that data protection officers from large companies made up a disproportionately large number of the participants. This can be attributed to the data collection methodology. The survey was addressed to data protection officers known by name, which is why companies without a data protection officer were left out.

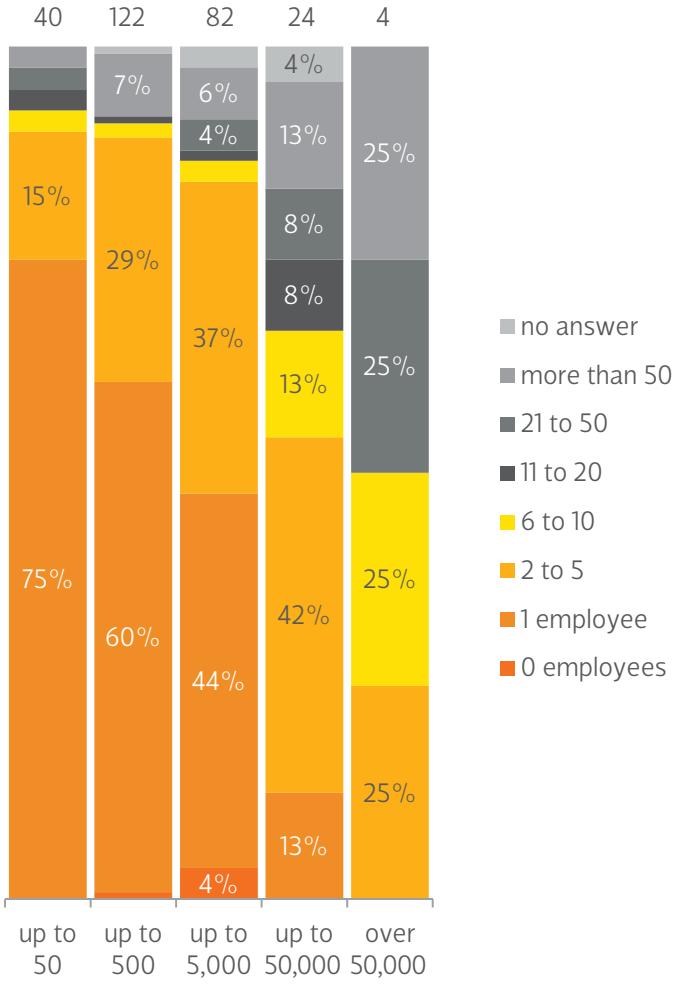
5. How many employees does your company employ across Germany?



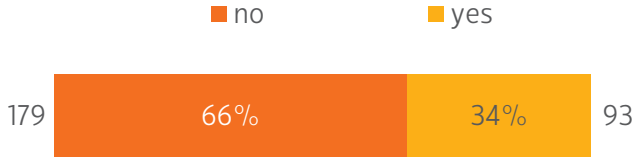
Across Germany, 15% of the participating companies employ up to 50 employees, 45% up to 500, 30% up to 5,000, 9% up to 50,000 and 1% over 50,000, such that the entire range of business sizes is represented in the sample group.

6. How many employees work directly with data protection in your company, in the sense that they contribute towards compliance with the precepts of data protection law?

Of the total of 960 employees worldwide and 1,006 in Germany who work directly with data protection in the participating companies, there are on average 5.24 and 3.9 employees per company respectively. The distributions of employees across the different classes of business sizes appears as follows:



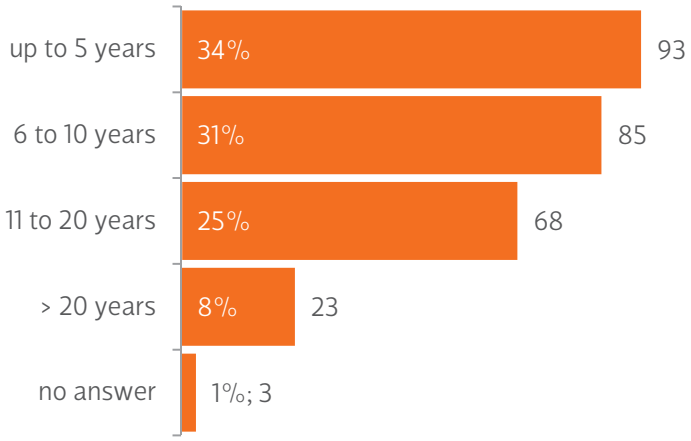
7. Is your company subordinated to a parent company?



66% of all businesses questioned are not incorporated into a parent company. Nevertheless, this indicates that almost a third of all data protection officers questioned face the issues of data protection within a corporate group.

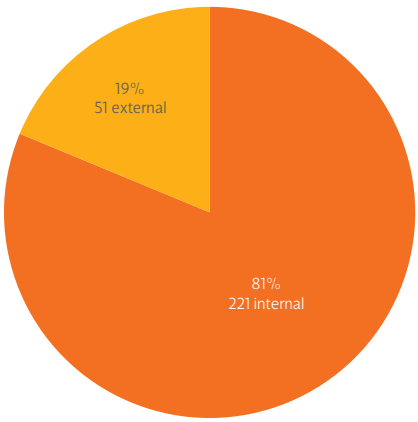
4.2 Data Protection Practice Within the Company

1. For how many years has your company had an appointed data protection officer?



In the companies questioned, the average length of time in which a data protection officer has been active is 17.7 years. The obligation to appoint a data protection officer was established in German data protection law as early as 1977 by the BDSG as a means of internal self-monitoring. The 2009 revisions extended the regulations to include a special protection from dismissal, thereby ensuring not only a technical justification but also legal grounds for employing the appointed data protection officers for an extended period. If one compares the size categories of the companies with the periods of appointment in each, it can be seen that efforts have been made since the BDSG revisions of 2009 in the smaller companies (up to 50 employees) to catch up with the obligation to appoint a data protection officer. Larger companies have generally employed data protection officers for a significantly longer time. The larger the company, the longer they have had data protection officers in place.

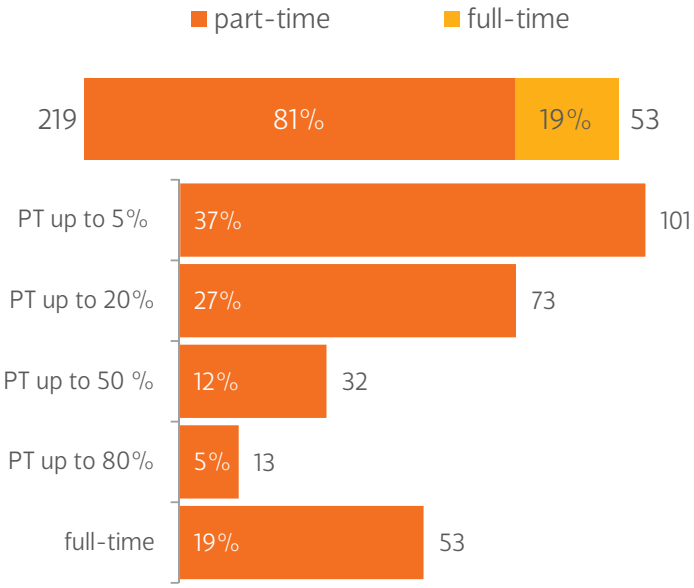
2. Are you employed as an in-house data protection officer or do you operate externally?



The BDSG offers the possibility of satisfying the general legal requirement of appointing an employee as an (internal) data protection officer by appointing an external data protection officer (section 4 para. 2 sentence 3 of the BDSG). This may be any person outside the data controller role – thus, either external specialist providers or other (internal) data protection officers of related companies.

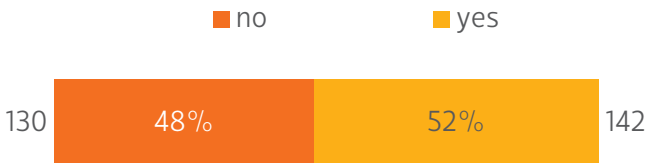
The number of internal and external data protection officers in our survey did not, however, give a representative picture of the distribution among the totality of German businesses, but rather the composition of the group of respondents. In practice, companies generally employ an internal data protection officer: 81% of the companies have appointed data protection officers from their own staff. The other 19% of companies have taken advantage of the option of appointing external data protection officers.

3. How much of your work time is devoted to your duties as the data protection officer?



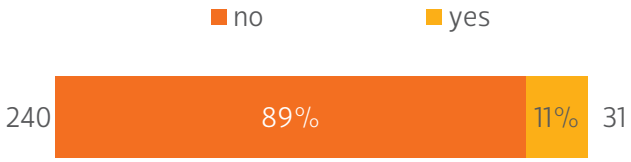
The legal prerequisite governing the legitimacy of the appointment of a data protection officer is his or her suitability for fulfilling his or her duties. This includes the granting of sufficient work time. With the decision of the Düsseldorfer Kreis from November 24-25, 2010, the highest regulatory authorities in Germany formulated the minimum requirements for the expertise and independence of data protection officers under section 4f para. 2 and 3 of the Federal Data Protection Act (BDSG) but did not specify the time requirement in more detail. The utilization and workload of data protection officers is principally influenced by the size of the responsible company, the number of companies worked for,, the particularities of data processing in the particular industry and the level of protection required for the personal data to be processed. According to the outcomes of the study, 81% of data protection officers work part-time and 19% full-time. This proportion has not changed since 2012. The part-time group has, therefore, been questioned in greater detail in the 2015 study. This has shown that 37% of the part-time data protection officers devote up to 5% of their work time to data protection issues.

4. Do you consider the amount of time available to you for carrying out your duties to be sufficient?



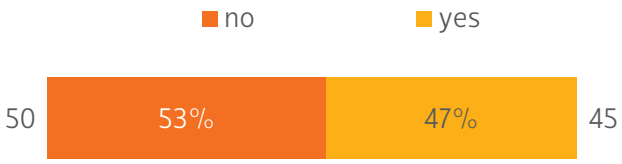
Just over half of the data protection officers questioned (52%) consider the time available to them to be satisfactory. From this it can be concluded that 48% of the data protection officers questioned believe that their appointment does not satisfy the requirements of the Data Protection Act. If insufficient time is available, a data protection officer is regarded as not effectively appointed. Apart from the restricted effectiveness of the work itself, this also means a heightened risk of fines being imposed.

5. Is your company subject to the obligation to report under section 4d para. 4 BDSG (commercial data processing for purposes of transfer, anonymized transfer or market research and opinion polls)?



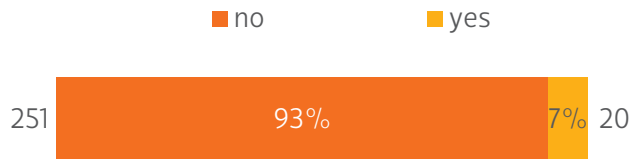
Under section 4 of the BDSG, the obligation to report automated data processing activities to the competent regulatory authority does not apply as long as the company has appointed a data protection officer. Yet, even if such an officer has been appointed under section 4d para. 4 of the BDSG, the competent regulatory authority must still be notified of the processes if they concern automated processing operations in which personal data is stored on a commercial basis for the purposes of transfer, transfer in anonymous form or market or opinion research. These notifications are held in registers by the appropriate regulatory authorities. Here it appears that an important condition for the registration of such processes is the appointment of a data protection officer who is in a position to implement the legal requirements in the company. 11% of the data protection officers questioned stated that their company is subject to the obligation to report. Compared to the results for 2012, in which 30% of companies were obliged to report, it appears that a reassessment has taken place in the last two years.

6. Do you meet the obligation to report?



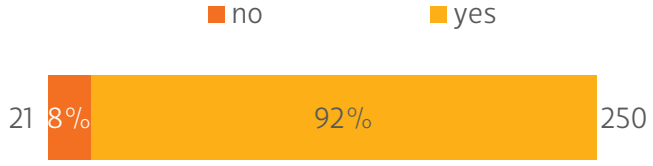
We added this question for the survey conducted in 2014 to examine the evident discrepancy between the obligation to report and the figures held by the regulatory authorities. Despite knowing about this statutory requirement, only 47% of the companies meet the obligation. Under section 43 of the BDSG, any organization that "intentionally or through negligence, contrary to Section 4d (1), also in conjunction with Section 4e second sentence of this Act, fails to submit a notification, fails to do so within the prescribed time limit or fails to provide complete particulars" is acting in breach of the statute. This carries a risk of fines that should not be underestimated.

7. Has your company been audited by a regulatory authority for data protection in the last two years?



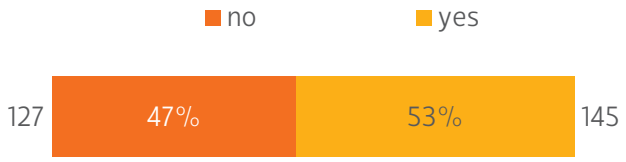
The sheer discrepancy between the number of staff in the regulatory authorities and the number of companies leads one to expect only a tiny fraction of respondents to reply in the affirmative. This would certainly also be the case in a representative survey of all companies. In the present survey, however, the responses have been primarily from appointed data protection officers in larger companies – so, evidently increasing the probability of prior experience with audits by regulatory authorities. It is also possible that the notion of an "audit" was not understood by all respondents in the same way. Actions such as questioning on certain legally prescribed elements in a large number of companies by individual regulatory authorities may in itself be regarded by some of the individuals questioned as auditing. Overall, 7% of the companies questioned have already been audited by a regulatory authority. This remains very low compared to the figure obtained in 2012 (15%). The reasons for the audits included complaints by data subjects (52%), no reason (33%), or automated audits, such as of a company's website, by the regulatory authority (14%). The situation remains unchanged that 35% (far above the average) of companies employing over 50,000 have experience with audits conducted by the regulatory authorities.

8. In your role as data protection officer, do you report directly to management?



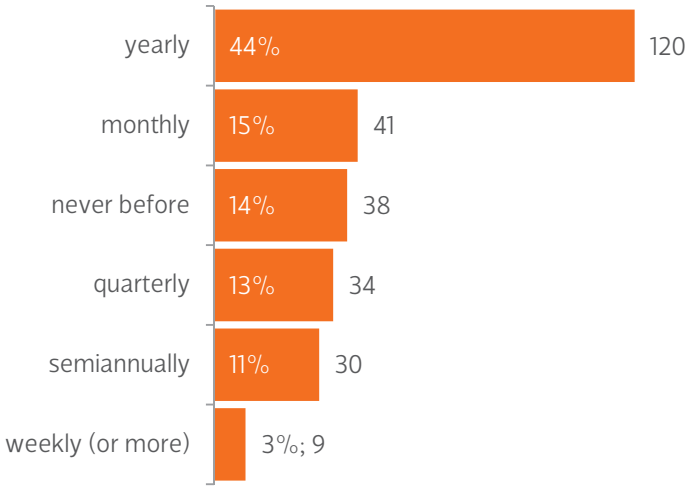
It is a mandatory legal requirement under section 4f para. 3 of the BDSG that the data protection officer report to the head of the data controller. Nevertheless, 8% of the data protection officers questioned answered this question with "no." This figure has increased in comparison to the results from "Data Protection Practice 2012", in which 4% of the data protection officers answered, "No."

9. Does your management require an activities report from you?



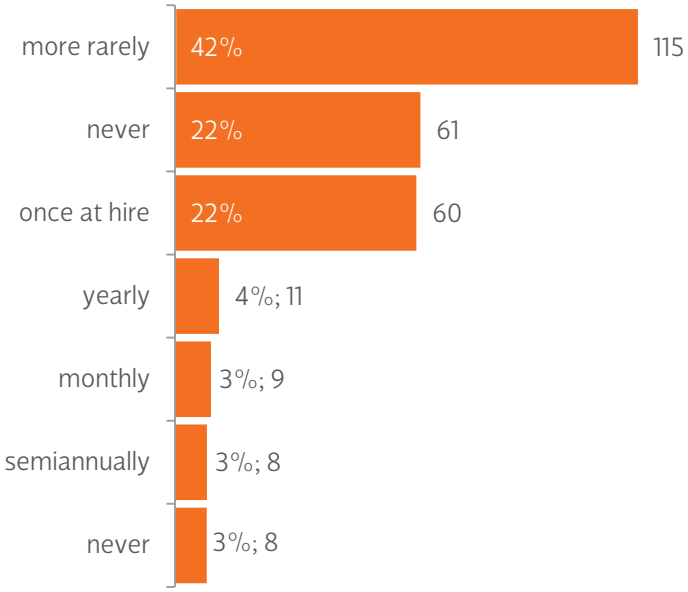
Unlike state data protection commissioners, who are obligated to Parliament as heads of regulatory authorities, no activity report by in-company data protection officers is required by law. Such reports have, however, proved to be a reliable tool for guiding the implementation of data protection regulations. Despite having appointed a data protection officer, the management still holds full responsibility even in this area. 53% of manageres ask for a report of this type. This result is surprising when compared with the results of the 2012 survey.

10. At what intervals do you report, orally or in writing, to management?



Just under half of the data protection officers report back to management annually (44%); only 14% have never reported to management so far. Each one of all 38 data protection officers who responded with "never" to the question of their obligation to report to management have also never been asked by management to submit such a report. In all other cases, the data protection officers produce a report, although they are not requested to do so. It can be seen from this that the data protection officers find it difficult to meet their responsibilities in the company unless they document their own work and report to management on a regular basis. The frequency of reporting changes only insignificantly when the management requests it. It is evident that the frequency of reporting is determined by operational practices and other internal reporting systems. The size of the company also does not appear to have a significant effect on the frequency of reporting.

11. How often are your company's employees normally given training in data protection?

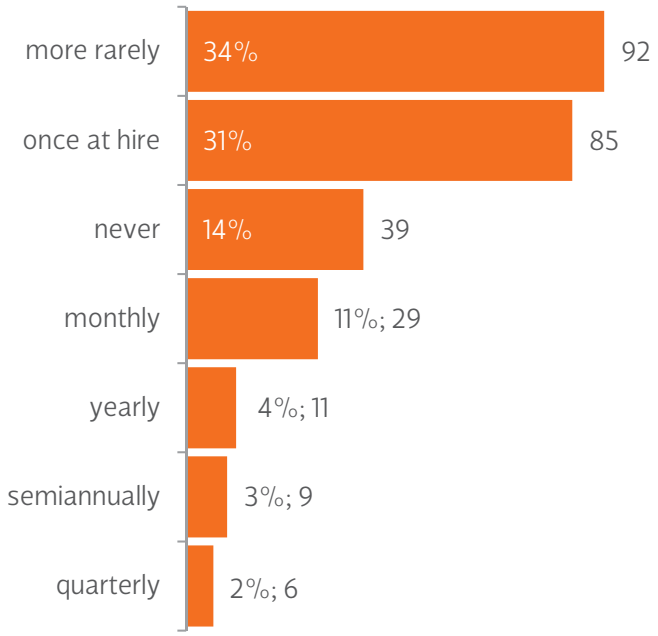


The core legal tasks of the data protection officer include familiarizing employees with the data protection provisions and with the various special requirements of data protection, section 4g para. 1 point 2 of the BDSG. The manner and extent of this training depend on the specific conditions of the company and the particular positions held by the employees.

The extent, frequency and type of such training is decided by the data protection officer in his or her own capacity. 22% of the companies train their employees only once in data protection, which is during their induction. This can be lawful in certain areas in which the processing of personal data takes place occasionally at most, and not electronically.

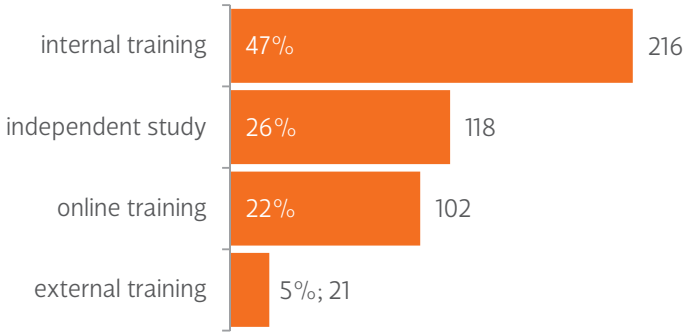
Only 4% of companies offer annual training for employees. A shorter training frequency (monthly or bi-annually) may be necessary in sensitive areas and is practiced in 9% of the companies. The majority of employees (42%) were, however, given training less often than annually. Compared to "Data Protection Practice 2012," this picture has changed remarkably. At that time the majority (39%) of data protection professionals stated that their employees were trained annually. This picture has to be corrected now. Clearly the need for training is not being met.

12. How often are your company's employees given specialist training in data protection (face-to-face training, e-learning, web-based training) with specific content such as data processing for marketing or in the personnel department?



In addition to general training in the Data Protection Act, the statutory duties of the data protecion officer include "familiarizing employees with the various special requirements of data protection," section 4g para. 1 point 2 of the BDSG. 31% of employees have only been given specialist training in data protection once, during induction, while 20% receive training annually or more often and 34% less frequently than annually. By contrast, 14% of employees have never been trained. Compared to the result in "Data Protection Practice 2012," a negative trend can be seen here. Then the data protection professionals stated that 48% of employees were trained yearly or more often and only 6% had never received training. This tendency is surprising since the need for employee training in the light of constantly changing work content and technical and organizational requirements is continuing to grow.

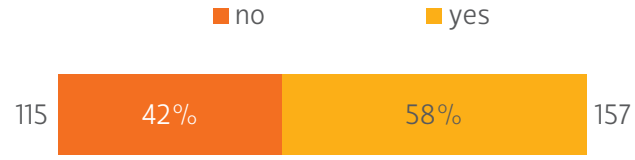
13. What methods do you use for training your company's employees?



Employee training is one of the core duties of the data protection officer. The majority of data protection officers run internal data protection training (47%), while only 5% work along with external providers; nevertheless, 22% of the data protection officers at least make use of online training aids. 26% of employees train using self-study methods. This weighting has changed little compared to "Data Protection Practice 2012."

4.3 Data Protection Breaches Within the Company

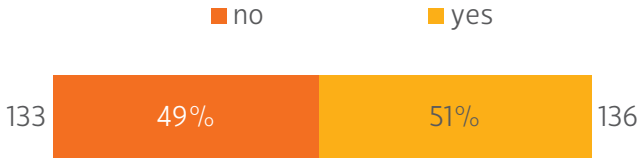
1. Do you feel satisfactorily informed about possible breaches of data protection due to security violations in your company?



In-company data protection breaches not only harm the company's image but can result in information obligations and claims for damages by affected parties. In certain cases, they must also be reported to the responsible regulatory authority under section 42a of the BDSG. At the same time, such violations form an important source of information for the data protection officer, enabling him to meet his obligations to implement the data protection legislation. In any event, the data protection officer must be informed of any breach and must be involved in its resolution.

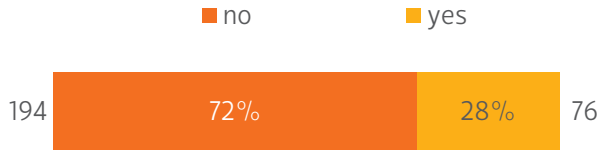
42% of the in-company data protection officers feel insufficiently informed of data protection violations in their company. Considering that the respondent group consists largely of data protection officers with many years of experience, this large proportion, representing a slight increase over the result from "Data Protection Practice 2012" (38%), is cause for alarm.

2. Do you feel that you are informed in a timely manner about possible data protection breaches caused by security violations in your company?



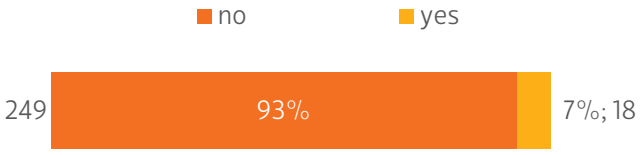
Only 51% of data protection officers stated that they have been informed of potential breaches of data protection in a timely manner. This is a cause for concern given the current need for action in response to data protection breaches. Possible problems can occur due to too little involvement of the data protection officer in projects, in particular in the planning phase. Only the involvement of the data protection officer at an early stage can facilitate the evaluation of possible information obligations under Section 42a of the BDSG in a timely manner.

3. Have you ever had to clarify whether a notification under section 42a of the BDSG (information obligation in the case of possible unlawful disclosure of data by third parties) is necessary?



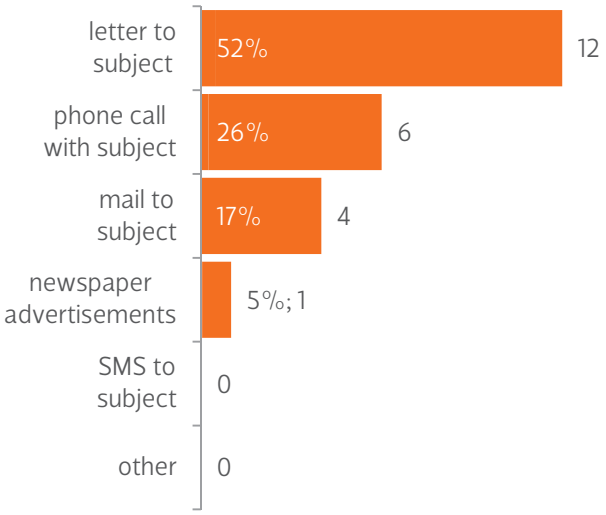
Section 42a of the Federal Data Protection Act (BDSG, Bundesdatenschutzgesetz) postulates an obligation to notify the responsible person or office in the event of unlawful acquisition of personal data by a third party if this threatens serious harm to the rights or legitimate interests of those affected. This relatively new regulation in the BDSG has caused much uncertainty in the practice and the need for clarification. The results of the survey give clear proof of the relevance of such assessments, where on average 28% of the data protection officers questioned have already had to carry out such an assessment. Growing relevance can also be seen by comparing this with the results of "Data Protection Practice 2012." Back then, only 21% of data protection officers stated that they had already had to carry out an assessment of this kind.

4.1 Have you ever had to submit notifications under section 42a of the BDSG?



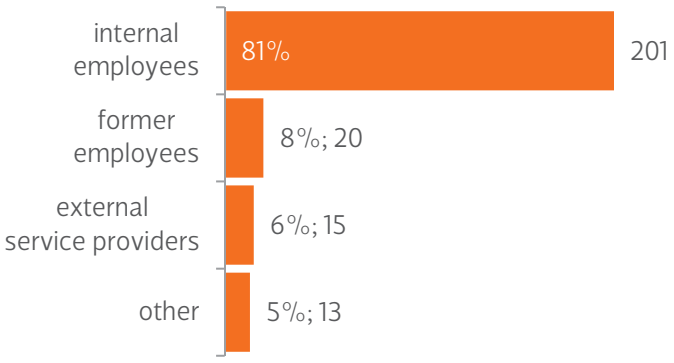
Under section 42a of the BDSG, there is an obligation to notify the competent authority in the event of personal data being unlawfully obtained by a third party if this threatens serious harm to the rights or legitimate interests of the data subjects affected. If such a risk is detected, the affected data subjects must be informed and given a description of the nature of the unlawful disclosure and recommendations of measures to minimize possible harm. Such a notification is made by the data controller. Compared to the survey results of the "Data Protection Practice 2012" (5%), the number of notifications required under section 42a of the BDSG has increased slightly (7%).

4.2 In what form have you provided information under section 42a of the BDSG?



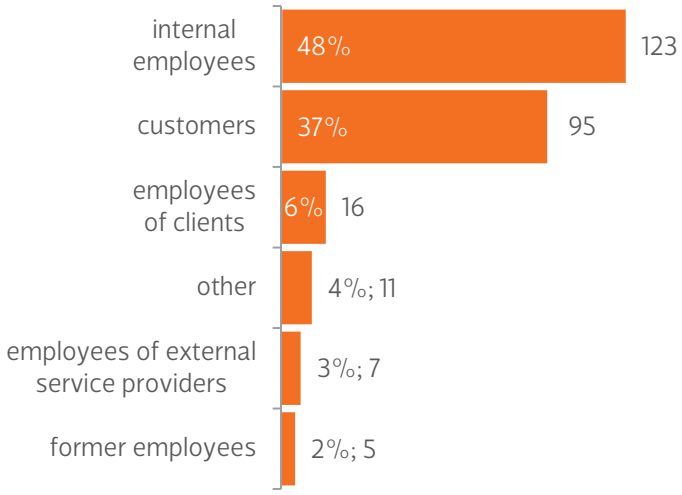
In these 23 cases, notification was issued to the affected parties under section 42a of the BDSG mainly (52%) by letter, in 26% of cases by a telephone call, in 17% of cases by e-mail and in 5% of cases by announcements in newspapers.

5. Which group, in your view, causes the largest number of data protection breaches in your company?



Data protection law governs the protection of personal data from abuse by unauthorized parties. In the experience of the data protection officers, the most serious cause of data privacy violations is misconduct on the part of individual employees (81% of responses). Only 6% of the responses implicate external service providers and a further 5% indicate other perpetrators. As could be seen in "Data Protection Practice 2012" results, the views of the data protection officers give distinct emphasis to internal perpetrators. Two years ago, individual employees also formed the most frequently cited group at 60%.

6. Which group, in your view, is most frequently affected by data protection breaches in your company?



The victims of data protection breaches are the data subjects whose data is processed unlawfully. In a company this could be either customers or the company's own employees. Compared to the results for "Data Protection Practice 2012," customers are no longer the most affected by breaches (37%); instead, the most frequent victims are the company's own employees (48%). These figures suggest an equal weighting of self-monitoring under data protection law between external victims (customers) and internal victims (employees).

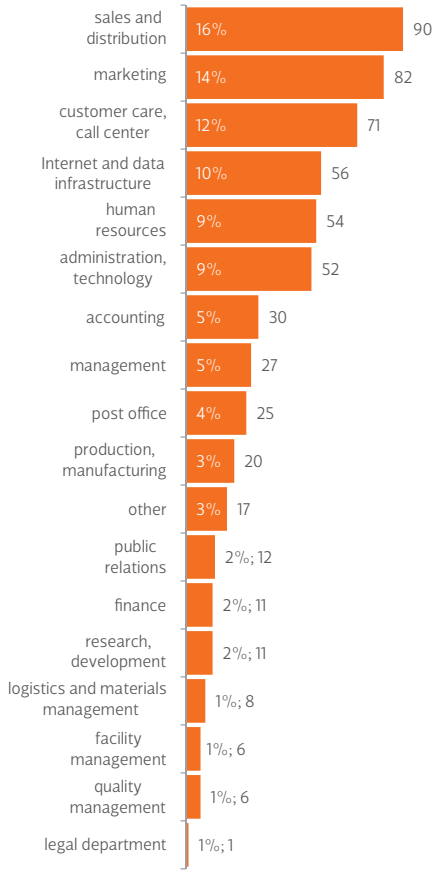
7. Evaluate the frequency of the following causes of data protection breaches in your company.

Reason	Frequent	Fairly frequent	Fairly rare	Rare	Never
Negligence	20.00%	38.11%	21.13%	16.60%	4.15%
Total	58.11%		41.89%		
Ignorance	10.15%	36.47%	29.32%	19.92%	4.14%
Total	46.62%		53.38%		
IT infrastructure	3.41%	13.64%	28.03%	43.18%	11.74%
Total	17.05%		82.95%		
Corporate guidelines	3.88%	11.24%	12.79%	34.88%	37.21%
Total	15.12%		84.88%		

The survey gave negligence, ignorance, IT infrastructure and corporate guidelines as possible causes. The data protection officers questioned are, however, divided over the importance of "negligence" as a cause of data protection breaches: while 58% experience this "frequently" or "fairly frequently," the other 42% rated this cause between "rare" and "never." "Ignorance" comes out only slightly more clearly as a cause: here roughly 47% of the data protection officers considered it a frequent occurrence, while 53% evaluated it between fairly rare and never.

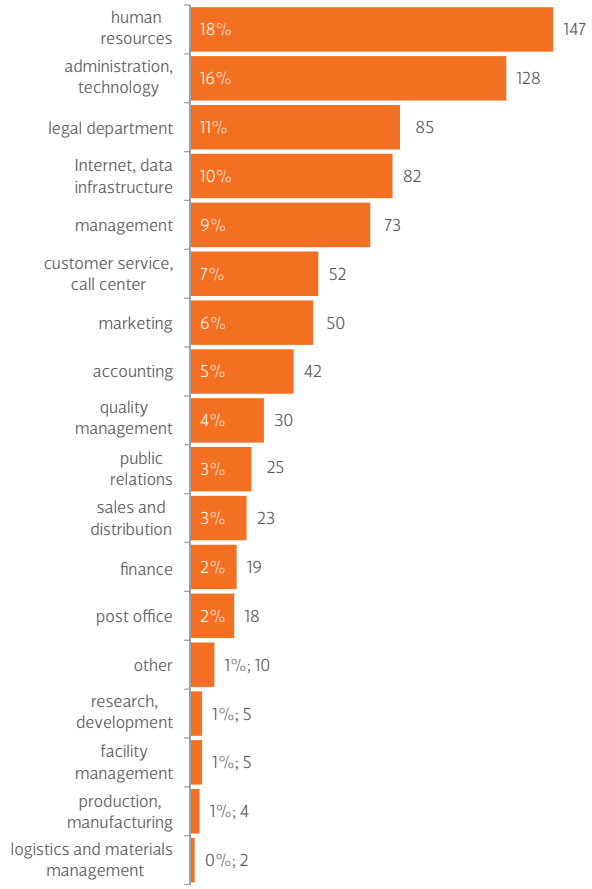
The picture becomes clearer only with "IT infrastructure" and "corporate guidelines": 83% and 85% of respondents rated these as "rarely" or "never" a cause for data protection violations. This analysis underlines the need for employee training as an effective means for combating the most significant cause of data protection breaches.

8. In which departments do you observe the most data protection breaches?



Sales, distribution, marketing and customer support are not only the departments that contain the largest amount of personal data. They also remain in 2014, as in 2012, at the forefront of data protection breaches.

9. In which departments, in your view, are the most effort directed towards data protection?



It can be seen from the results that awareness is highly variable between departements. While personnel departments are most concerned with data protection issues, they are still in fifth place for violations. The worst offenders for data protection violations are the sales, distribution and marketing departments. These same departments also come last when it comes to addressing data protection issues. Here, as also in "Data Protection Practice 2012," the expected relationship between ignorance of the legal regulations and data protection violations can be clearly seen.

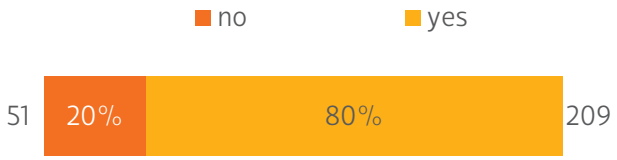
10. How often do you observe the data protection breaches in the list below in your company?

	Frequent	Fairly frequent	Fairly rare	Rare	Never
Unauthorized entry to operational work areas	2.64%	10.94%	22.64%	39.25%	24.53%
Total	13.58%		86.42%		
Careless handling of IT infrastructure	5.97%	33.21%	25.37%	27.61%	7.84%
Total	39.18%		60.82%		
Unauthorized use of EDP equipment	1.50%	8.24%	22.85%	33.33%	34.08%
Total	9.74%		90.26%		
Unlawful collection of personal data	5.24%	20.97%	29.21%	26.97%	17.60%
Total	26.22%		73.78%		
Unauthorized processing of personal data	3.33%	21.85%	28.15%	28.15%	18.52%
Total	25.19%		74.81%		
Unlawful transfer of personal data	3.76%	17.29%	25.19%	30.08%	23.68%
Total	21.05%		78.95%		
Data processing in violation of contract	1.15%	6.90%	18.39%	38.31%	35.25%
Total	8.05%		91.95%		
Improper storage of personal data	4.51%	21.05%	24.81%	33.83%	15.79%
Total	25.56%		74.44%		
Documents left in printers	6.74%	20.60%	27.72%	35.21%	9.74%
Total	27.34%		72.66%		
Unencrypted, unsecured IT and EDP equipment	11.19%	22.01%	20.52%	30.97%	15.30%
Total	33.21%		66.79%		

Data protection breaches are as many and varied within companies as their possible causes. The law distinguishes more formal violations, which can be fined up to €50,000, from substantive violations, which involve an infringement on the rights to informational self-determination of the data subjects and may be fined by up to €300,000. Violations committed with deliberate intent for financial gain or to cause harm may be punished with up to two years imprisonment. The survey posed questions about typical data protection breaches in practical experience.

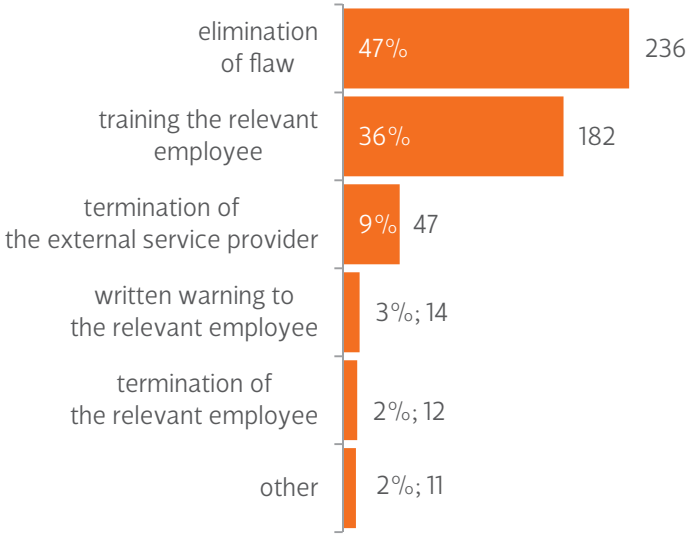
These related both to typical misconduct by employees (carelessness, unauthorized use, improper storage, documents left lying about), and also to insufficient implementation of the legally prescribed organizational measures (unlawful data collection and transfer and the processing of personal data in violation of contract and without authorization) as well as technical actions (unencrypted or unsecured IT and electronic data processing equipment). In order of frequency of responses, careless use of IT infrastructure, unencrypted or unsecured IT and EDP equipment and documents left in printers were the most common data privacy violations in the companies questioned. Processing personal data in violation of contract, on the other hand, was the least frequent violation.

11. Did your management undertake corrective action after the discovery of a data protection breach?



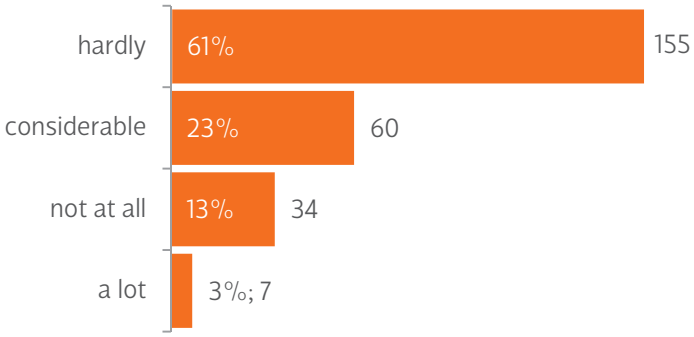
The experience of the data protection officers questioned is that 80% of the detected data protection breaches were also suitably punished. By contrast, in "Data Protection Practice 2012" the data protection officers stated that barely half (49%) of all data protection breaches went unpunished after discovery.

12. What were the consequences to which the detection of a data protection breach led?



47% of data protection officers stated that, in their experience, the consequences of discovering a breach of data protection extended only to remedying the fault. Other corrective action frequently included training for employees (36%) to prevent future data protection breaches. Less frequently, more drastic actions were taken – the employees in question were disciplined (9%), fired (3%) or the service provider's contract was terminated (2%).

13. How satisfied are you with the consequences?



In-company data protection officers are not authorized to punish violations of data protection law, nor do they have any obligation to report violations to the competent regulatory authority. Here they are reliant on the company management and its willingness to take action in response to violations and misconduct.

In those cases in which detected data protection breaches were punished, 74% of responses from the data protection officers questioned were "hardly" or "not at all" satisfied with the consequences. Such dissatisfaction can perhaps be explained by the consequences being too slight (47% stated that these consisted solely of rectifying the fault). This result is surprising when it is compared with the results of the 2012 survey. At that time the majority (63%) of the data protection officers responded that they were "fairly" or "very" satisfied with the corrective action taken.

4.4 The Data Protection Officer in the Company

1. How many clients (companies) do you support in addition to this company in the capacity of data protection officer?

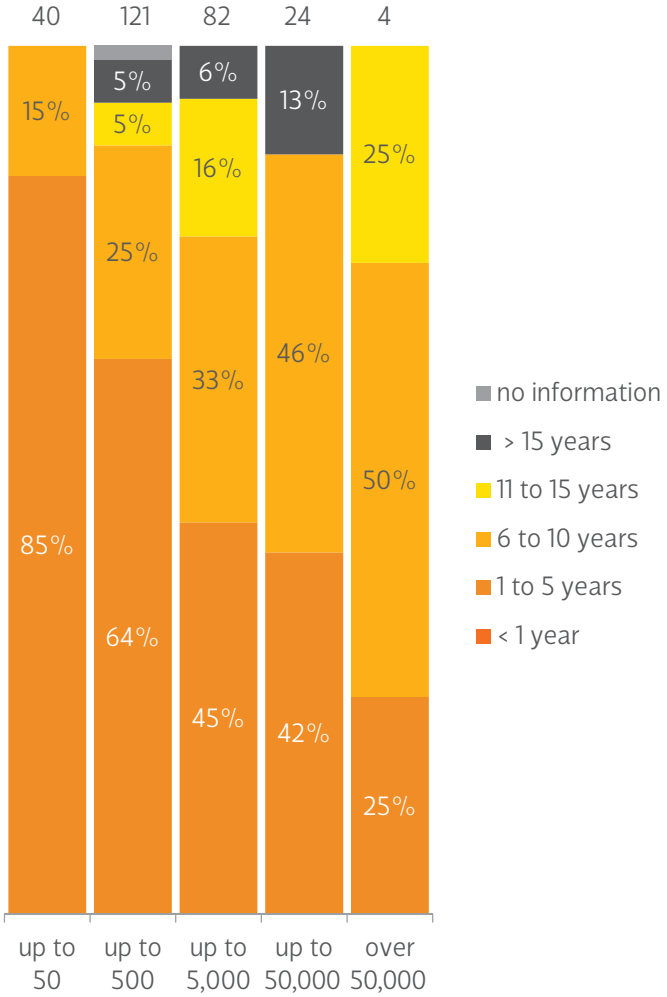
The study collected the number of companies and of employees on average over the last two years. 159 of the respondents do not work for any other company as an external data protection officer. 112 data protection officers support a total of 658 further companies (on average 5.8 companies per head) with a total of 31,028 employees (on average 277 per officer).

This question makes it easier to interpret the results of the 2012 survey: Of the 63 external data protection officers who participated in the 2012 study, nine (14%) now support only one other customer; in 2014 this applied to 29 out of 112 (25%).

In 2012, 38 of the respondents (60%) supported between two and 10 other companies; in 2014 this was 66 (59%). In 2012, seven of the data protection officers questioned (11%) supported a further 11 to 20 clients; in 2014 this was 18 (16% of respondents).

One respondent claimed in the 2014 survey to support 50 other companies with 600 employees. This officer had, however, a budget of €1.1 million and 8.5 more employees at his disposal.

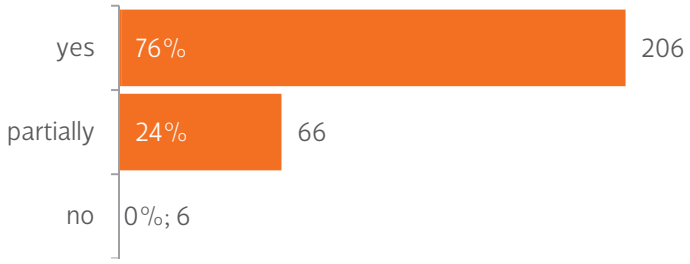
2. How long have you been employed in your company as a data protection officer?



In total, the 263 data protection officers who responded to this question have been gathering data protection experience for 1,602 years in the same company, which results in an average time of 5.9 years in the position.

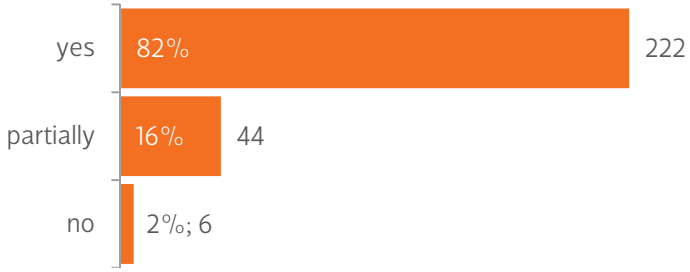
Looking at the time in a position in relation to the size of the company in which the data protection officers work, it is noticeable that the length of time in the position is correlated with company size. Generally speaking, data protection officers of larger companies have been in the position for a longer time.

3. Are you known to all the employees in your company as the data protection officer?



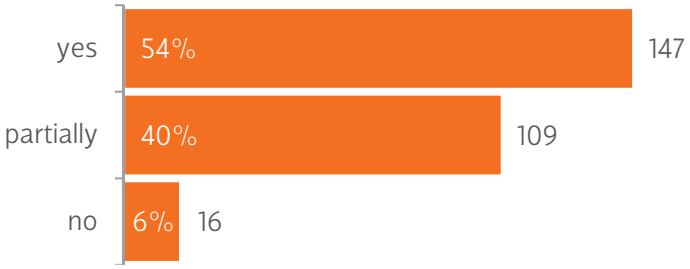
Because of the data protection officer's function on the one hand as an expert advisor and on the other as an appeals authority for employees in the event of data protection violations, his or her being known as such in the company is, in most cases, a matter of course. 76% of the data protection professionals stated that they are known within their company as the data protection officer, while the remaining 24% said that they were at least partly known. In 2012, 86% of the data protection officers questioned stated that they were known in their companies, and only 13% were only partially known. From this, a shift can be seen in the structure of the participating data protection officers.

4. Are you able to pursue your duties as data protection officer in a professionally independent capacity?



Only 82% of the data protection officers suppose that they are able to pursue their job in a professionally independent capacity, although this independence is a mandatory requirement for the appointment to be legally effective. Possible causes of restrictions, drawn from evaluation of the results for questions 4.4.6 and 4.4.10, are that both support from management and support from personnel were rated to some extent as unsatisfactory.

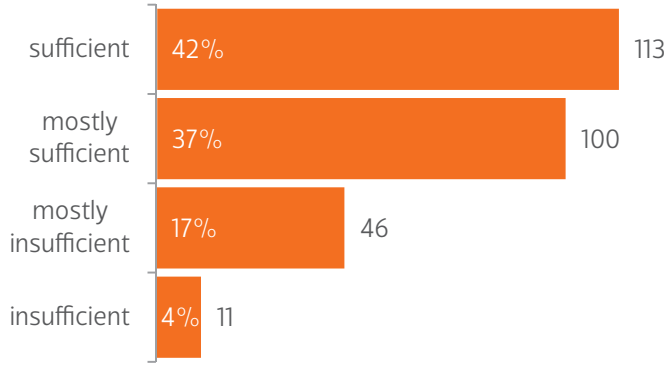
5. In your view, does the management meet its obligations in respect to internal data protection management?



Participants were questioned with regard to space provided, time and assisting personnel, the availability of training and the bearing of the costs of training, as well as support provided to data protection officers through the designation of contact persons in the departments.

About half of the data protection officers (54%) stated that, in their view, the management fulfilled their obligations in respect to internal data protection management; another 40% stated that the management did so to some extent. Possible reasons for the remaining 6% to answer with "no" to this question may be deduced from the evaluation of results from the questions that follow. Reasons for complaint included poor support from management and from other personnel and the lack of involvement of the data protection officer in projects.

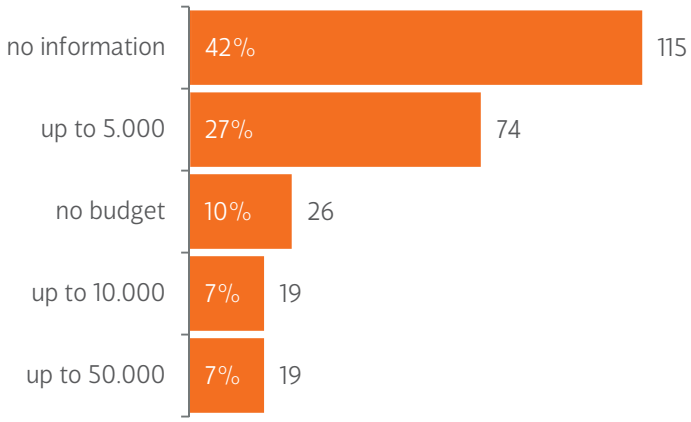
6. How do you rate the support for your work as data protection officer given by the management?



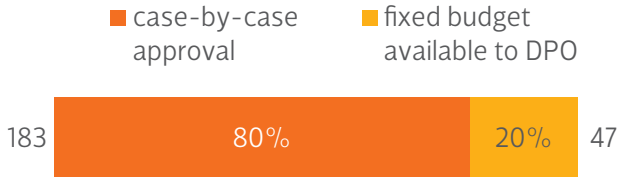
Nevertheless, 21% of data protection officers questioned rated the support received for their work by the management as "unsatisfactory" or "fairly unsatisfactory," while 79% rated the support as "satisfactory" or "fairly satisfactory." An improvement can, however, still be seen here compared to the responses to this question in "Data Protection Practice 2012." At that time, 33% evaluated support by management as unsatisfactory.

7.1. How much budget is available to you annually for your work as a data protecion officer?

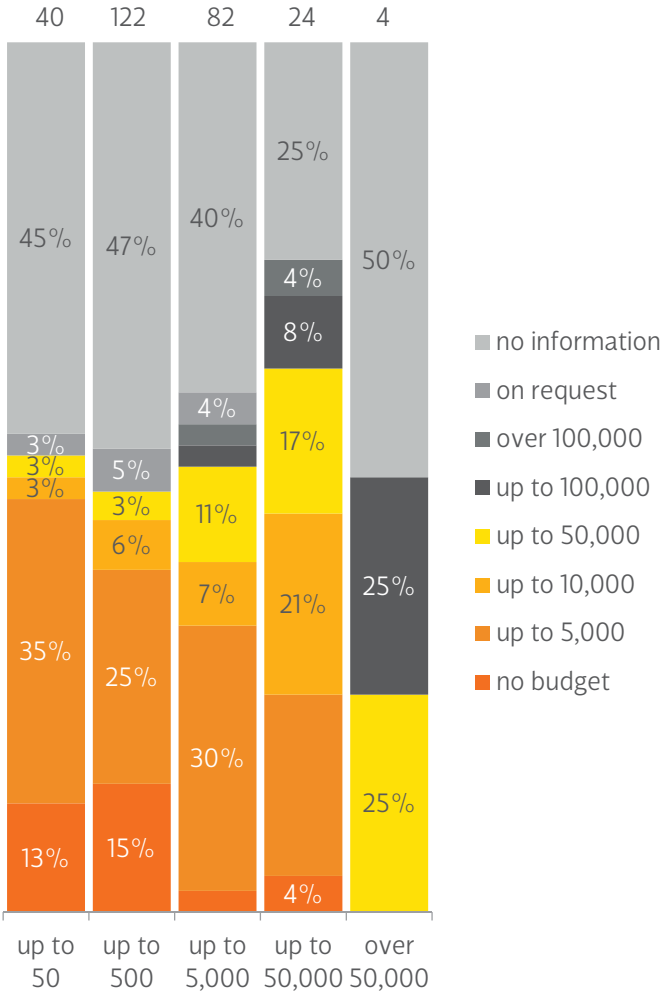
Excluding any personnel costs or other internal settlements.



7.2 In what form can you access this budget?



7.3 How high is the budget of a data protection officer according to company size?



The average annual budget of the data protection officers who replied to this question is €18,822. Thanks to the concretization of this question, the result appears more realistic than it did in "Data Protection Practice 2012," where the budget stated by the data protection officers was on average €70,596. Evidently, in 2012, most data protection officers included personnel costs in the budget.

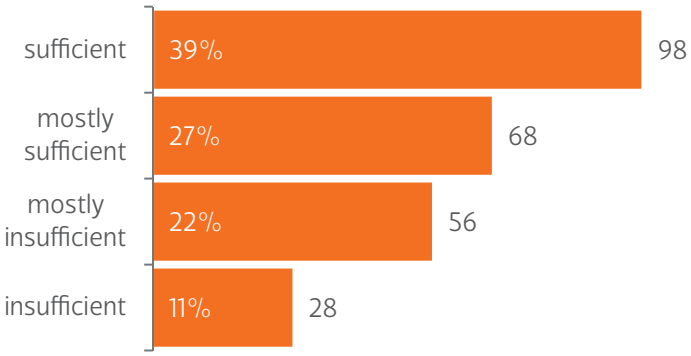
10% of the data protection officers questioned stated that no budget was available to them; the question was answered by only 156 officers in total.

In the second part of the question, it can be seen that the significant majority of data protection officers (80%) can receive their budget on request, as expected.

The size of the budget also increases with company size. It should, however, be noted that this result is not representative, since the number of responses to the question (only 156 out of 272 data protection officers questioned) is too small.

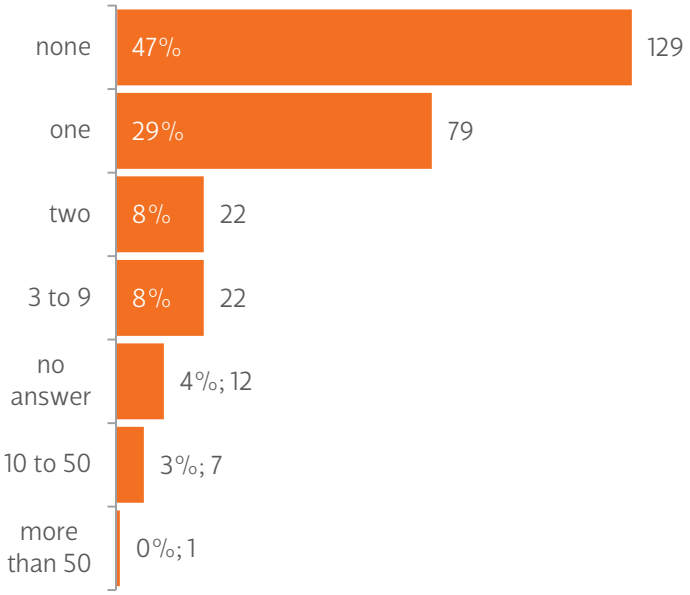
The low percentage values of the "majorities" can be explained because the missing responses from the remaining 115 data protection officers have been integrated into the statistics as "no response." Generally, companies with up to 50 employees are allotted a budget of up to €5,000 (35%); companies with up to 500 employees are allotted up to €5,000 (25%) or up to €10,000 (6%); companies with up to 5,000 employees generally receive a budget of up to €5,000 (30%), up to €10,000 (7%) or up to €50,000 (11%). In larger companies with up to 50,000 employees, the budget is normally up to €5,000 (21%), up to €10,000 (21%) or up to €50,000 (17%). In companies with over 50,000 employees, the budget is normally up to €50,000 or up to €100,000.

8. How do you assess the size of this budget?



Similarly to the case in "Data Protection Practice 2012," the majority (66%) of the data protection officers questioned rated their budget as "satisfactory" or "fairly satisfactory."

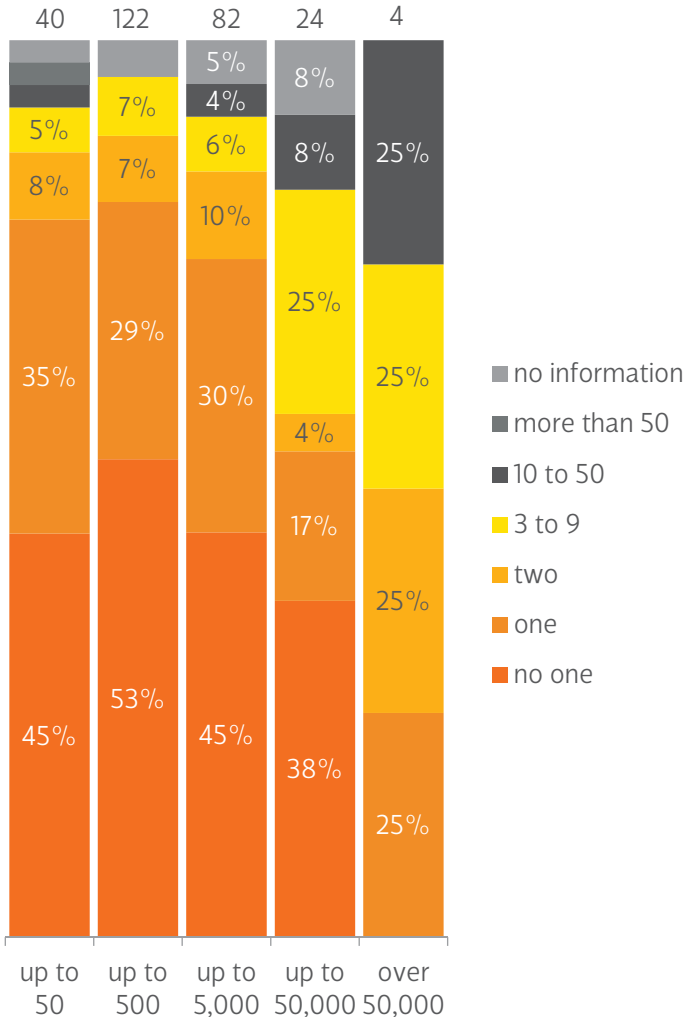
9. How many employees are, for the purposes of fulfilling your duties, directly available to you as expressly named contacts, assistants or parts of the data protection organization?



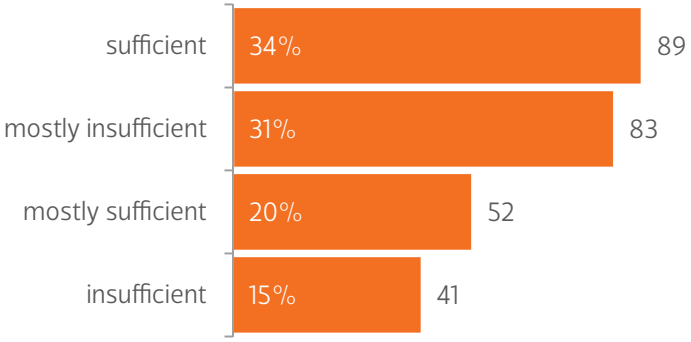
261 data protection officers questioned stated that they had an average of 1.7 staff available to them directly for carrying out their

duties. This is, nevertheless, 30% more employees available for support, on average, than was reported in "Data Protection Practice 2012" results. It, nevertheless, continues to confirm the image of the data protection officer as acting single-handedly in the company.

The following table clarifies the relationship between the number of data protection staff and company size in Germany:



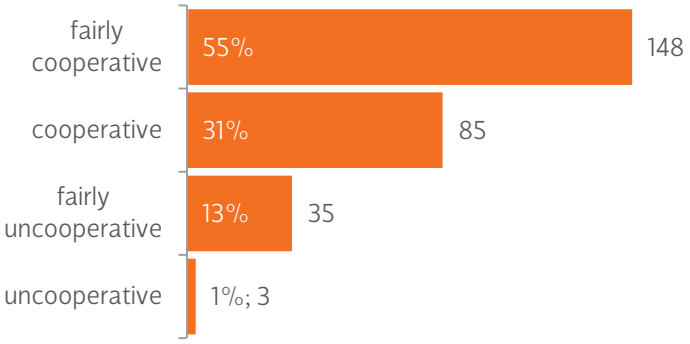
10. How do you rate the personnel support you receive?



54% of the data protection officers, nevertheless, consider the support of available personnel to be "satisfactory" or "fairly satisfactory" for the fulfillment of their duties. However, 46% of the data protection officers are not satisfied.

Although they have 1.7 more employees each at their deployment and, therefore, 30% more support than they had according to the results of "Data Protection Practice 2012," more data protection officers rated their personnel support as either "fairly unsatisfactory" or "unsatisfactory" in 2014.

11. How cooperative do you find the company departments in working with data protection?



As was the case in 2012, the vast majority of data protection officers see the specialized departments in the company as cooperative. This response also reflects the particular situation in the companies questioned, in which the data protection officer has often been in that role for many years.

12. Please rank the following areas of expertise for your work in order of importance:

1: most – 6: least

	Average
Audit, review	3.53
Business management	4.70
Data protection law	1.63
IT security	2.31
Communication	2.85
Organization	3.09

In the ranking of the expertise required for the function of data protection officers, data protection law unsurprisingly remains in first place (average score 1.63), followed closely by issues of IT security (2.31), knowledge of in-company communications (2.85) and organization (3.09). Knowledge of auditing (3.53) and

business management (4.7) were regarded by the respondents as the least important. The rated value of knowledge of data protection law has however improved from 2.18 in 2012 to 1.63, which highlights an increasing level of juridification in the field.

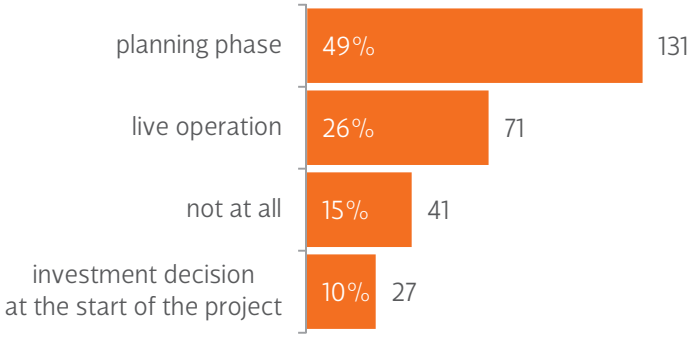
13. Please arrange these activities in the order of how much time they take you:

1: most – 6: least

	Average
Requests from employees	3.26
Consultancy to management	3.78
Performing training	3.56
Requests from external data subjects	5.40
Internal audits and inspections	3.62
Monitoring of contract data processors	4.16
Privacy inventory tool	3.68

The ranking of time demands on data protection officers is led by internal requests (3.26), followed by provision of training (3.56), auditing and checks (3.62) upkeep of the privacy inventory tool (3.68) and providing consultancy to management (3.78). The least time is taken up by auditing contract data processors (4.16) and external requests (5.4). This result allows one to suppose that persons outside the company who are affected by data breaches are hardly aware of the possibility of complaints to the in-company data protection officer, or certainly make little use of it. This weighting corresponds to the outcome of this question in "Data Protection Practice 2012".

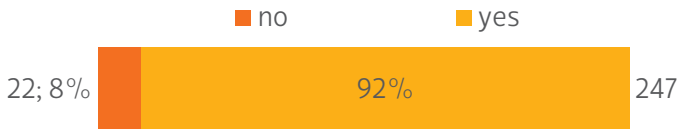
14. In what phase do you normally become involved in projects?



Only involvement of the data protection officer at an early stage can prevent wrong decisions and bad investments. 49% of data protection officers stated that they become involved at the project planning phase to assess the project's implications in respect to data protection law; 10% become involved in the investment decision when the project commences, and 26% only become involved once the project is under way. A further 15% of data protection officers are never involved in projects at all.

4.5 The Privacy Inventory Tool

1. Is a privacy inventory tool used in your company?

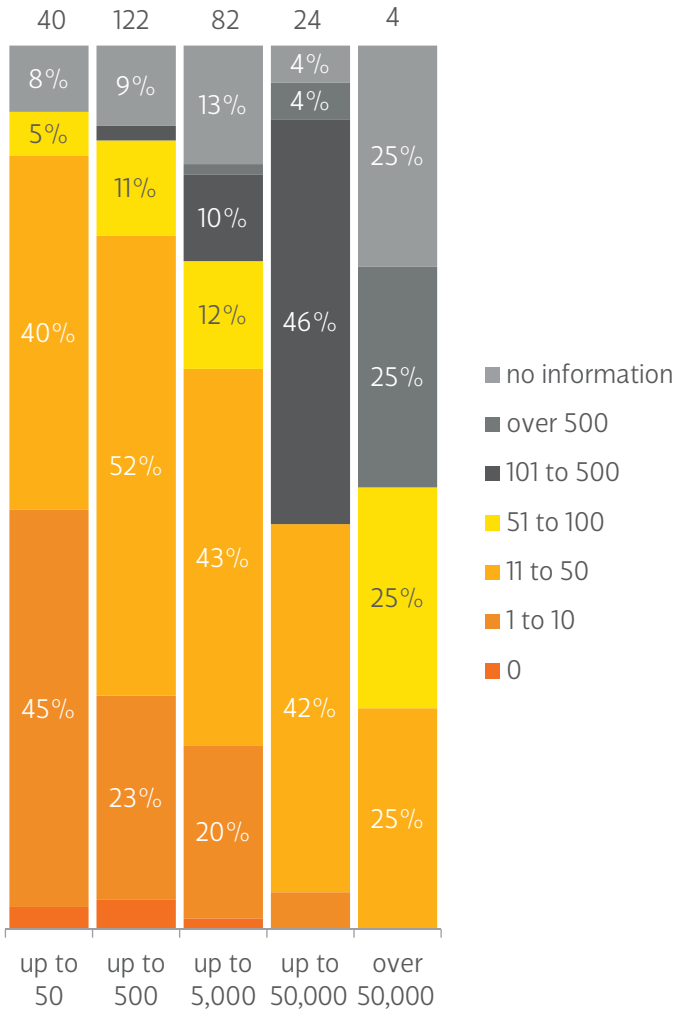


8% of the data protection officers questioned still stated that the company does not maintain a privacy inventory tool. Since it is highly unlikely, with the current use of automated data processing systems, that companies will not process personal data in some automated form, the absence of a privacy inventory tool under section 4g para. 2 of the BDSG constitutes an infringement of the company's obligations, because this inventory must be made available to the data protection officer.

The consequences of the lack of a privacy inventory tool are various. Neither can the data protection officer make the public part of the inventory available to any person who requests it, as is required by law, nor is he in a position to verify whether a given procedure is subject to a prior check. He does not have the overview of the data processing procedures used by the company, which makes his task consultation on deletion, correction or information requests considerably more difficult.

While the absence of a privacy inventory tool does not mean the imminent threat of a fine, the lack of the tool can allow illicit procedures to take place undetected and may, thus, lead indirectly to preventable difficulties for the company.

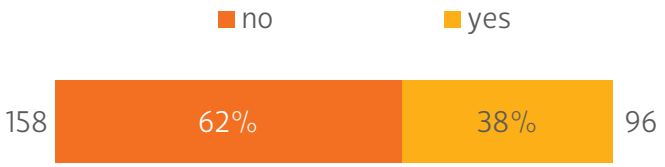
2. How many procedures are entered into your privacy inventory tool?



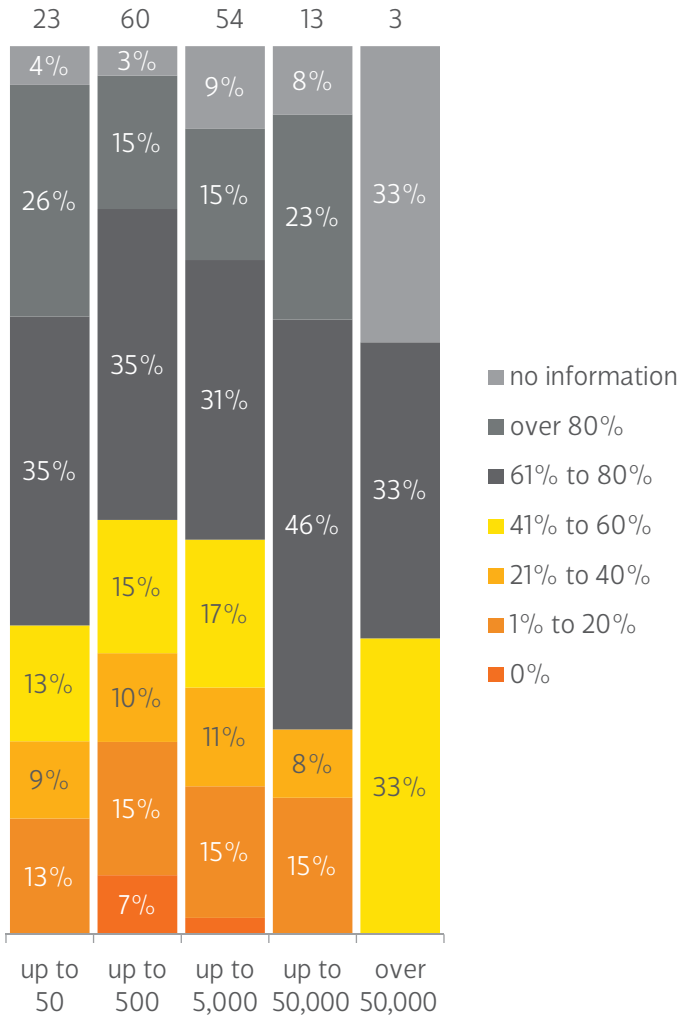
In the overview of all automated processes, the data controller, the group of data subjects affected, the type of data, the intended purpose and the data security precautions in particular are to be documented. When asked about the number of individual procedures within one processing overview, the data privacy officers gave an average of 57 procedures. Naturally, this number varies considerably with the size of the company. Thus, 25% of data protection officers in companies with over 50,000 employees stated that their privacy inventory tool covered more than 500 individual procedures.

These figures make it clear that maintaining the inventory is a substantial piece of work in organizational terms that requires significant resources. Among the companies with under 50 employees, by contrast, almost 90% of privacy inventory tools contain no more than 50 different procedures.

3.1 Are all your company's procedures recorded in the inventory?



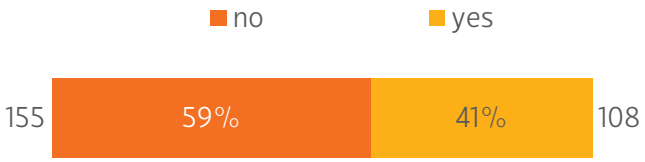
3.2 What percentage of procedures are recorded in it?



Only 38% of the data protection officers questioned stated that all their company's procedures were recorded in the privacy inventory tool. However, since an overview of all automated procedures must be complete, the absence of procedures from the privacy inventory tool constitutes a breach of the company's obligations under section 4g para. 2 of the BDSG. The respondents who replied that their privacy inventory tool was incomplete were then asked percentage of completion of the privacy inventory tool, in order to gain a clearer understanding. On average, a degree of completeness of about 60% was reported. To capture any particularities relating to the different company sizes, the completeness percentages of the privacy inventory were categorized by the number of employees in the company.

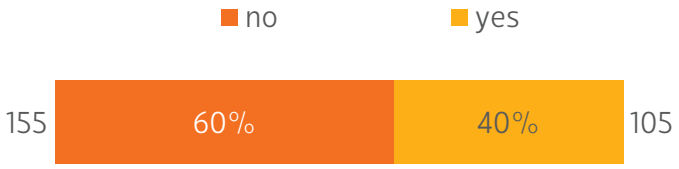
No particularities were detected in terms of company size. The largest or second largest category represented the average in every company size with a degree of completeness of 61-80%. Because of the small size of the sample, however, these results cannot be regarded as representative.

4. Is there an established process that ensures that the privacy inventory tool is up to date?



The privacy inventory tool is subject to constant change, due both to every modification made within the processes described in it and also changes to the technical and organizational procedures in the company. To ensure that the inventory tool is kept up-to-date, an internal process within the company is required. According to the responses of the data protection officers, 108 out of 263 companies (41%) have introduced such a process.

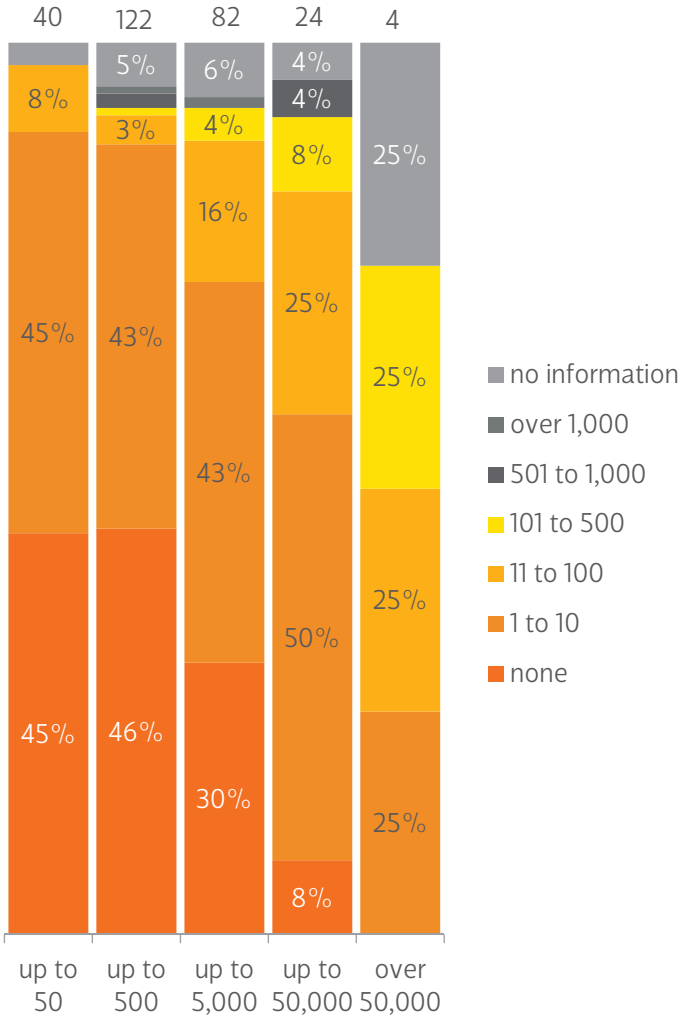
5. Does your company provide you with a privacy inventory tool, as required by law?



Under the BDSG regulations, it is the duty of the company to make an overview of automated data processing procedures (the "privacy inventory tool") available to the data protection officer. In practice, however, it often happens that when a data protection officer is first appointed, he or she must create the privacy inventory tool him or herself. 60% of the data protection officers answered this question in the negative, which, by a comparison to the response to question 4.5.1, makes it clear that the privacy inventory tool was not in fact created by the company and submitted to the data protection officer, as the law states, but rather was prepared by the data protection officer him or herself. Because of the high demands on the privacy inventory tool, however, it may in fact be advantageous for the data protection officer to be closely involved in the process after all.

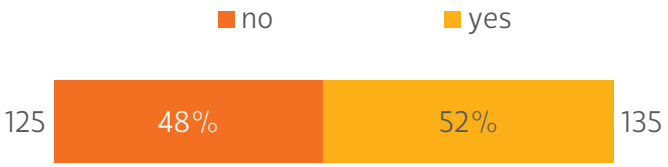
When compared with the results of this question in "Data Protection Practice 2012," the picture that emerges is surprising. In 2012, 28% of the data protection officers questioned answered with "no" to this question. This year, that figure has increased by 32% to 60%. This indicates that in 2012 the question was not yet formulated in sufficiently concrete terms. At that time, we asked whether the company provided a processing overview. Some of the respondents interpreted this as making the overview available to anybody who wished to see it. By reformulating this question, it is now clear that the obligation of the company toward its own data protection officer is unsatisfied far more often than was feared in 2012.

6. How many information requests does your company receive from customers each year?



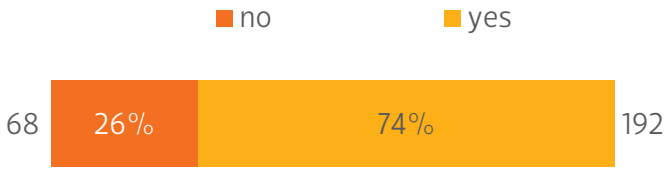
On average, the companies receive 231 information requests each year from customers. To capture any particularities relating to the different company sizes, the information requests per year were categorized by the number of employees in the company. As expected, it, thus, became clear that the number of information requests correlates with increasing company size.

7. Is there an established process for allowing members of the public to view the public part of the privacy inventory tool?



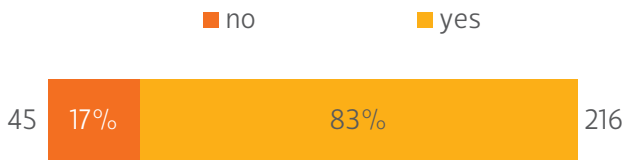
Although it is a duty of the data protection officer to make the public part of the privacy inventory tool available to any member of the public on request, there is an established process for this in only 52% of the respondents' companies. While failure to meet the obligation of making such a privacy inventory tool available to the public does not directly mean a penalty, it may be assumed that the persons who request such an inventory will be sufficiently aware of data protection issues to report any failure to provide an inventory to one or more regulatory authorities. This may then bring attention to other questions as well, such as that of an internal privacy inventory tool.

8. Are the company departments involved in creating and updating the privacy inventory tool?



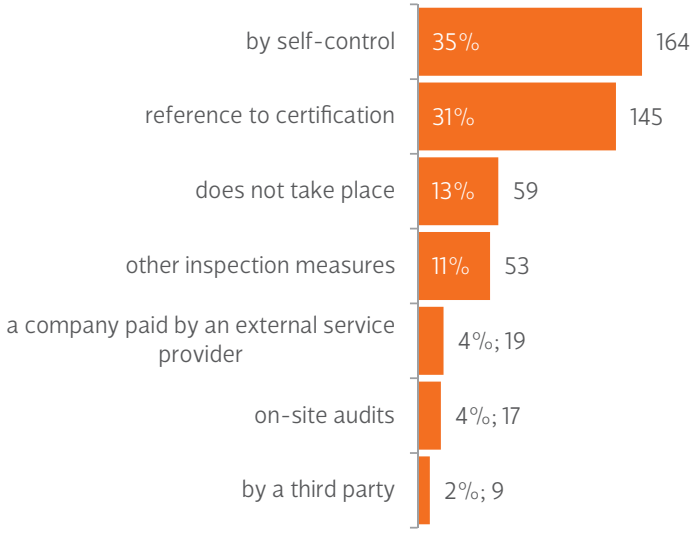
Similarly to the results in "Data Protection Practice 2012," only in 74% of the companies are the departments involved in creating and updating the process descriptions.

9. Do you compile the privacy inventory tool yourself?



The data protection officers questioned, who mostly have extensive experience in applying data privacy law, prefer in 83% of cases to prepare the privacy inventory tool themselves rather than having this done by the departments alone. Compared to "Data Protection Practice 2012," this significant majority has increased 23%, upward from 60%. This is clear confirmation of the tendency for data protection officers not to be mere "recipients"of the privacy inventory tools, as specified by the legislation, but rather to be actively involved in creating and maintaining them.

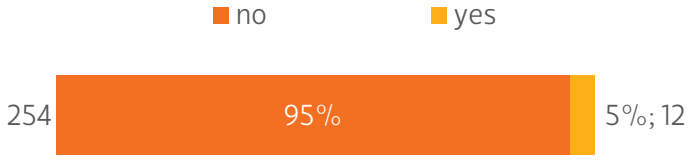
10. How do you, acting as a client, exercise the monitoring function when you outsource data processing to another party?



Under section 11 of the BDSG, the client remains legally responsible for data protection when he commissions a third party to process personal data. He has extensive inspection obligations which, however, he may exercise at his discretion. No specific form of monitoring is legally prescribed. Self-inspection (35%) and the number of certifications obtained (31% of all responses, up by 10% on the result for 2012) are among the inspection procedures stated most frequently. Despite the fact that the situation is clearly unlawful, 13% of respondents stated that no inspections were carried out. Only in a few cases were on-site audits carried out, either by service providers paid by the company or by independent third parties paid by the contractor.

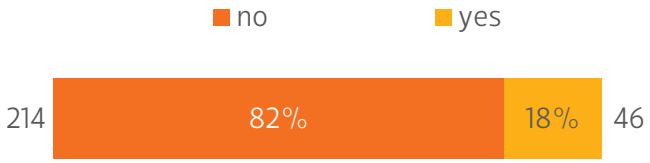
4.6 Certification

1. Has your company ever obtained data protection certification (e.g. EuroPriSe, ULD or similar, for products or services, procedures or company processes)?



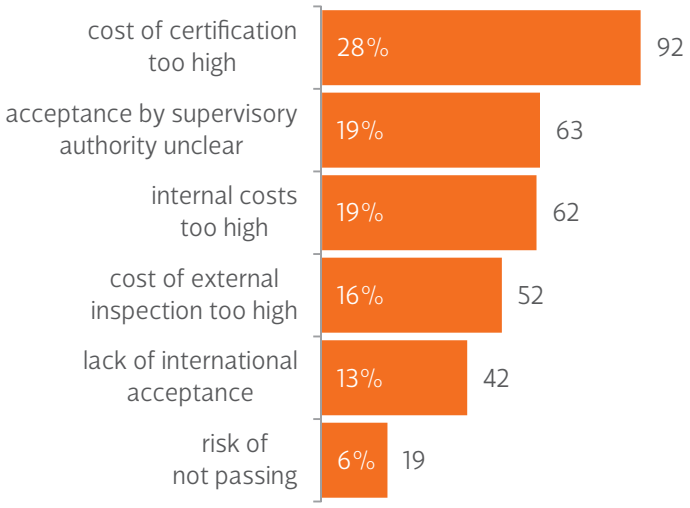
5% of the companies have had their own past experience with data protection certification. In 2012, this question was answered with "yes" by 7% of companies. The situation has, thus, not changed significantly.

2. Is your company interested in gaining data protection certification?



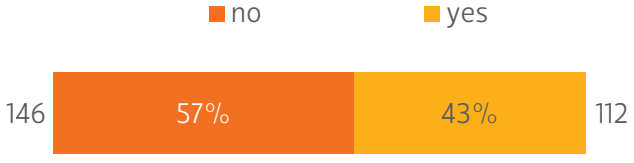
In 2014, 18% of data protection officers supposed that their company was interested in gaining data protection certification; in 2012, this figure was 21%.

3. If you have already taken a particular data protection certification into consideration, why was this not followed through?



Responses by the data protection professionals suggest that data protection certification was not ultimately obtained by their company primarily due to excessive costs (28% of all responses). Other reasons given were unclear acceptance by the regulatory authorities (19%), excessive internal costs (19%) and excessive costs of an external audit (16%). The least frequent responses given were lack of international acceptance (13%) and the risk of failing the audit (6%).

4. Do you consider data protection certification to be useful for your company?



Almost half (43%) of the data protection officers questioned would consider data protection certification as useful for their company. Considering the results of the survey for this question and questions 4.6.1 – 4.6.3, it is clear that, as expected, companies – or their data protection officers – are indeed interested and even take particular certification into consideration; however, most have not followed through with it, owing to excessively high costs.

4.7 Regulatory Authorities

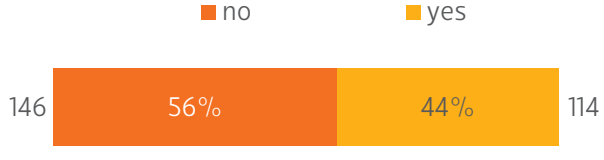
1. Please state your position on the following statements: Regulatory authorities...

	Agree	Tend to agree	Tend to disagree	Disagree	No opinion
Should audit more	16.09%	29.50%	25.67%	21.84%	6.90%
Total	45.59%		47.51%		
Should audit less	3.11%	12.06%	24.90%	48.64%	11.28%
Total	15.18%		73.54%		
Should act solely in an auditing capacity	5.43%	7.36%	20.93%	58.91%	7.36%
Total	12.79%		79.85%		
Should offer consulting/advice	54.75%	37.64%	4.18%	2.66%	0.76%
Total	92.40%		6.84%		
Should offer consulting and act as an auditor	44.27%	44.66%	7.63%	1.91%	1.53%
Total	88.93%		9.54%		
Should offer training	46.36%	29.89%	11.88%	10.73%	1.15%
Total	76.25%		22.60%		
Should offer certification	30.53%	31.68%	16.03%	15.27%	6.49%
Total	62.21%		31.30%		

Enthusiasm among data protection officers for inspections by the regulatory authorities is still limited; nevertheless, 46% of respondents would like more inspections. In almost complete agreement with this, the data protection officers demand more consultancy activity on the part of the regulatory authorities (92%) and for them to offer training (76%). Similarly, the majority (62%) of the data protection officers also demand certification through the regulatory authorities.

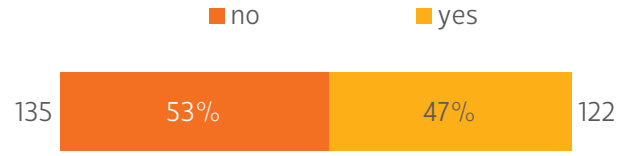
Compared to the responses to this question in "Data Protection Practice 2012," the tendencies in the various directions are now stronger and are more clearly pronounced.

2. Do you think that the actions taken by regulatory authorities are too inconsequential?



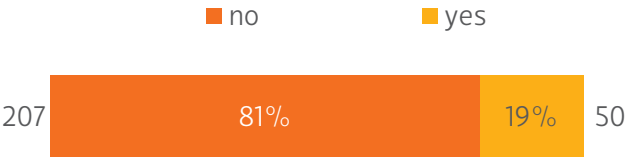
44% of the data protection officers questioned considered actions of regulatory authorities to be too inconsequential. Thus, a proportion of the respondents (11% greater than in 2012) regard the regulatory authorities as something of a "toothless tiger." This tendency should be a cause for concern for the regulatory authorities.

3. Do you believe that data protection breaches are sufficiently prosecuted by the regulatory authorities?



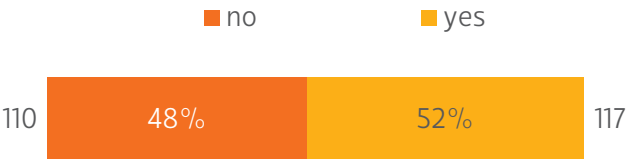
In the experience of 53% of the data protection officers, data protection breaches are not satisfactorily prosecuted by the regulatory authorities. This view is made clearer by comparison with "Data Protection Practice 2012" and when the results of the previous question are considered. Compared to the result in "Data Protection Practice 2012," this opinion has nonetheless increased by 5%. In question 4.7.2, 44% of the data protection professionals stated that in their view the regulatory authorities act too inconsequentially. Compared to "Data Protection Practice 2012," this figure has increased by a further 11%. To summarize, it can, thus, be said that the prosecution of data protection breaches by the regulatory authorities was rated by almost half the data protection officers as unsatisfactory and therefore as inconsequential.

4. Have you experienced a situation in which competitors violate data protection regulations, avoiding prosecution and, thereby, gaining a competitive advantage?



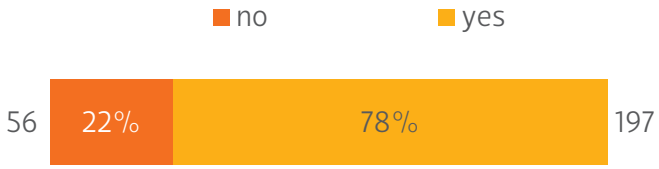
The majority of the data protection officers (81%) stated that, so far, they had not experienced such a situation (of a competitor violating data protection regulations, avoiding punishment and gaining a competitive advantage).

5. Do you consider the resultant penalties and fines as sufficient?



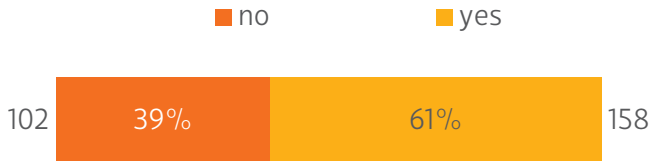
The penalties imposed by regulatory authorities for data protection breaches in companies are regarded by 52% of the data protection officers as sufficient.

6. Do you consider the regulatory authorities to be sufficiently competent?



22% of the data protection officers questioned still have doubts as to the competence of the regulatory authorities. Compared to 2012 (24.5%), this figure has fallen slightly, but only insignificantly. The doubts as to the competence of the regulatory authorities seem to be hardening.

7. Is the possibility of telephoning the regulatory authority for data protection taken seriously in your company?



Only 61% of the data protection officers questioned have the impression that the possibility of telephoning the regulatory authority is taken seriously within their company. Compared to the figure obtained in 2012, this figure has fallen substantially from 75%.

To summarize, the results contained in this chapter give a generally critical view of the regulatory authorities. They are criticized for lack of consistency, insufficient prosecution of data protection breaches and, in some cases, penalties and fines that are too small. Moreover, almost half of the data protection professionals in the study seek more auditing and more extensive information provision from the regulatory authority in the form of consulting and training.

4.8 Legal Issues

1. Please state your position on the following statements:

	Agree	Tend to agree	Tend to disagree	Disagree	No opinion
The data protection officer requires a form of authority.	36.12%	33.46%	12.17%	18.25%	0.00%
Total	69.58%		30.42%		
Data protection laws are comprehensible and unambiguous.	2.65%	20.45%	43.56%	33.33%	0.00%
Total	23.11%		76.89%		
It is possible to abide by all data protection laws.	3.41%	26.14%	35.61%	33.33%	1.52%
Total	29.55%		68.93%		

Almost 70% of the data protection officers argued in favor of their profession being given a form of authority to issue directives. The majority of the data protection officers regard the existing data privacy laws as neither comprehensible (77%) nor practical (69%). This confirms the results of the 2012 study.

2. Changes are needed in these areas:

	Agree	Tend to agree	Tend to disagree	Disagree	No opinion
Contract data processing	26.34%	32.44%	23.66%	11.83%	5.73%
Total	58.78%		35.50%		
Data protection for employees	38.02%	33.84%	17.11%	7.60%	3.42%
Total	71.86%		24.71%		
Data protection and advertising	22.01%	32.84%	21.27%	10.82%	13.06%
Total	54.85%		32.09%		
Transnational data flows	40.08%	29.18%	6.61%	2.33%	21.79%
Total	69.26%		8.95%		
Data protection on the Internet	44.23%	34.62%	8.46%	8.85%	3.85%
Total	78.85%		17.31%		
Personal Internet and e-mail use at work	40.46%	36.26%	14.50%	7.25%	1.53%
Total	76.72%		21.76%		
Video surveillance	23.85%	26.92%	25.77%	19.62%	3.85%
Total	50.77%		45.38%		

A large majority of the data protection officers, increased by 6% compared to the 2012 result, wish primarily to see changes in the law relating to online data protection (79%), personal Internet and e-mail use at work (77%) and data privacy for employees (72%). The data protection officers also see the need for action on the regulations on transborder data flows (69%) and on contract data processing (59%).

A slight majority of 55% also wanted changes in the area of data privacy and advertising. The general opinion about the need for action at the legislative level on video surveillance (51%) remains undecided.

3. In your view, do the existing laws cover the following topic areas adequately in practical terms?

	Agree	Tend to agree	Tend to disagree	Disagree	No opinion
Cloud computing	1.93%	8.11%	24.71%	59.46%	5.79%
Total	10.04%		84.17%		
Data processing within corporate group	2.70%	23.17%	23.94%	36.68%	13.51%
Total	25.87%		60.62%		
Geolocation	1.19%	11.07%	36.36%	32.02%	19.37%
Total	12.25%		68.38%		
International data processing	0.77%	9.62%	33.08%	40.00%	16.54%
Total	10.38%		73.08%		
Rights and obligations of data protection officer	14.29%	54.44%	22.01%	8.11%	1.16%
Total	68.73%		30.12%		
Social media	1.15%	8.85%	33.46%	52.31%	4.23%
Total	10.00%		85.77%		
Handling of customer data	8.08%	58.46%	23.46%	8.85%	1.15%
Total	66.54%		32.31%		
Video surveillance	7.69%	47.31%	28.08%	12.69%	4.23%
Total	55.00%		40.77%		
Advertising	1.93%	35.52%	34.75%	19.31%	8.49%
Total	37.45%		54.05%		

For the most part, the data protection officers questioned are satisfied only with the statutory regulations concerning the rights and obligations of the data protection officer. Only 30% see the need for correction here, while 32% see the need for corrections to the regulations for handling customer data. As for all the other areas of regulation questioned, disagreement rates up to 86% indicate a strongly negative view by the data protection officers.

Highest on the negative rankings were social media (86%), cloud computing (84%) and international data processing (73%), followed by geolocation (68%) and data processing within corporate groups, the regulations of which are considered by 61% to be in need of revision.

The opinion profile of the data protection officers reflects the public discussion very clearly: the new challenges to data protection law as a result of international networking represent a significant task for the legislature. Traditional data protection law seems unable to provide convincing answers for internationally networked communication.

As for so-called social media offerings, not only does the relationship between informational self-determination and commercial utilization of private communication come up against technical limits, but national regulations also come against the boundaries of services performed internationally.

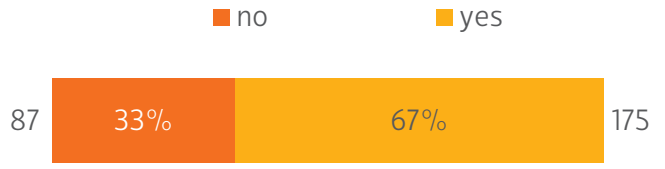
4. In which areas do you also see the need for legislation to catch up?

The participants had the opportunity of stating additional topics requiring legislative action in a free-text field. As well as the topics covered in the study, the total of 44 suggestions included repeated demands for clarification regarding the powers of the police and public prosecutor to act against criminal activity from companies. They also included demands for resolving the contradictions between data protection for employees and customers on the one hand and the compliance requirements of terrorism blacklists, authorized economic operator (AEO) certification and similar statutory requirements on the other.

Protection against domestic and foreign state surveillance was also identified here as an area in which the legislation should be updated.

4.9 Training of Data Protection Officers

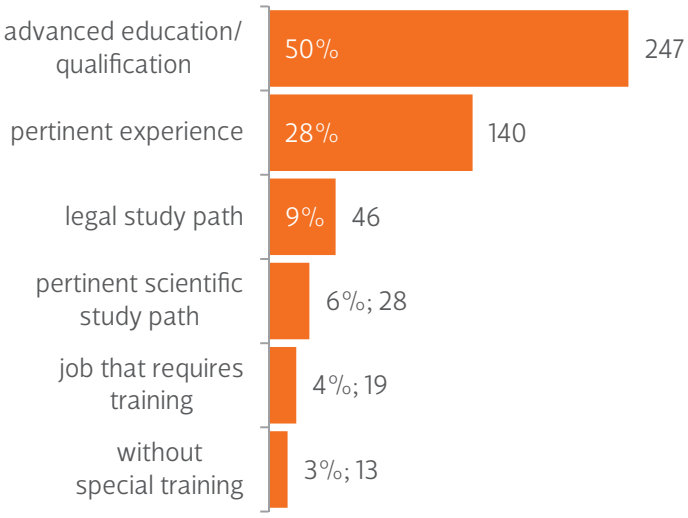
1. Would you consider a legally prescribed training for data protection officers as useful?



The BDSG sets out personal and technical requirements for the appointment of a data protection officer; these have been made concrete by a decision of the supreme regulatory authority. There exists no vocational training or professional qualification to date grounded in legislation. This deficiency is an issue of complaint not only for trainers and the professional association; 67% of respondents to the survey also argue for legally regulated training. This confirms the result for 2012 (64%).

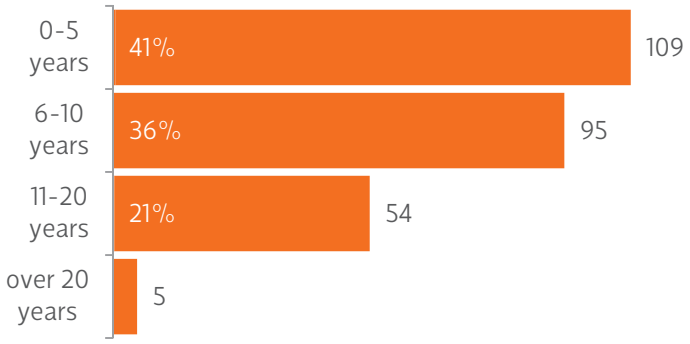
2. How did you become qualified as a data protection officer?

Multiple responses may be given.



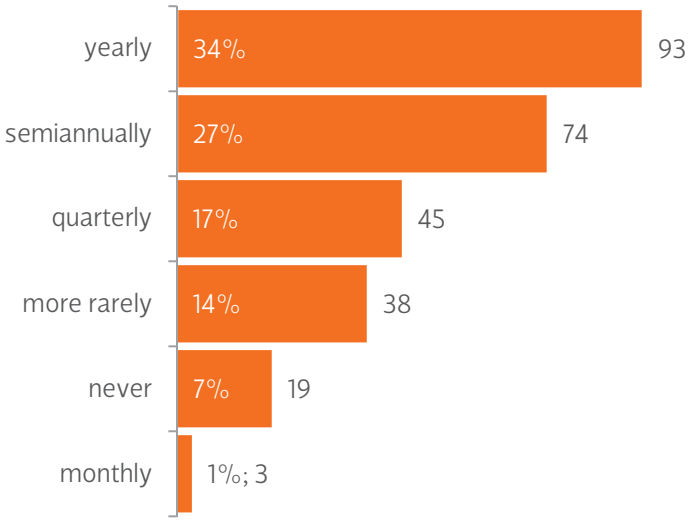
The professional qualification required in order to work as a data protection officer can be obtained in various ways, such as by studying engineering or law at degree level. These disciplines, however, provide only a basic competence, which must be complemented by suitable advanced training and continuing professional development (CPD). Various modular options spread over several weeks are available on the CPD market, as well as intensive courses lasting between one and five days. 50% of the participating data privacy officers stated that they gained their qualifications through continuing professional development measures; 28% rely on the experience they have gained in the course of their work and 15% rely on prior knowledge obtained from a course of study. These results demonstrate that the required qualifications are generally gained through CPD and experience gained on the job, and largely confirm the results of the 2012 study.

3. How long have you been working in data protection in general?



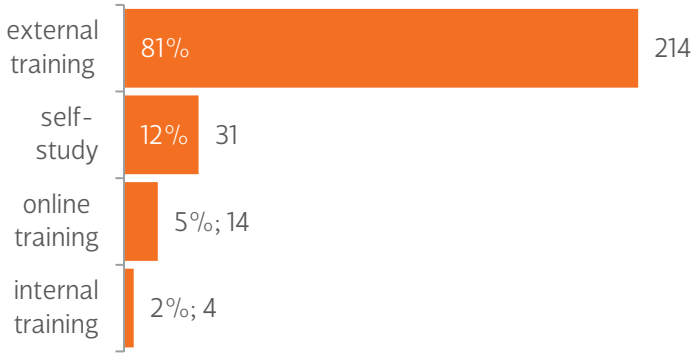
In Germany, there has been an obligation to appoint data protection officers since July 1, 1977. Failure to do so may result in fines. The data protection officers questioned stated that they had worked in data protection for an average of 7.9 years. 2% of respondents had worked in data protection for over 20 years; 21% had done so for between 11 and 20 years; and 36% had done so for between six and ten years. 41% of respondents had worked in data protection for less than five years. The sum of the participants' experience is, thus, 2,097 years.

4. How often, on average, do you participate in continuing professional development (CPD) events?



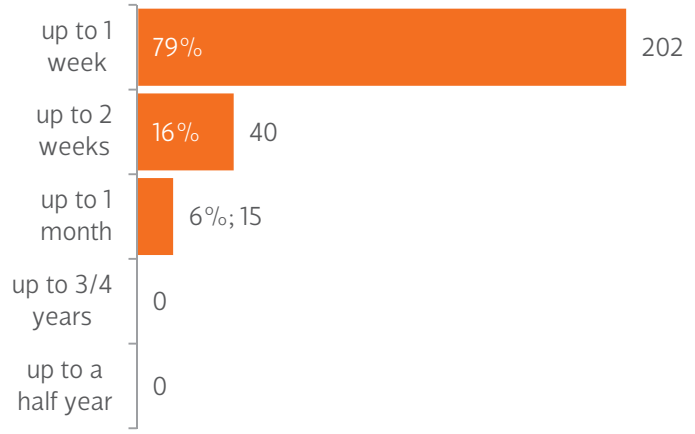
A particular challenge in the work of a data protection officer is not the complexity of the tasks in the company, but rather the continual changes in the legal framework and technical developments. Ongoing regular training (CPD) is therefore of particular importance in this profession. 17% of respondents avail themselves of CPD on a quarterly basis; 27% do so twice per year; and 34% do so annually. Overall, 79% of participants undertake some form of CPD at least once per year, while 14% do so less than once per year. Still, 19% of the data protection officers answered, "Never."

5. What is your preferred method of CPD?



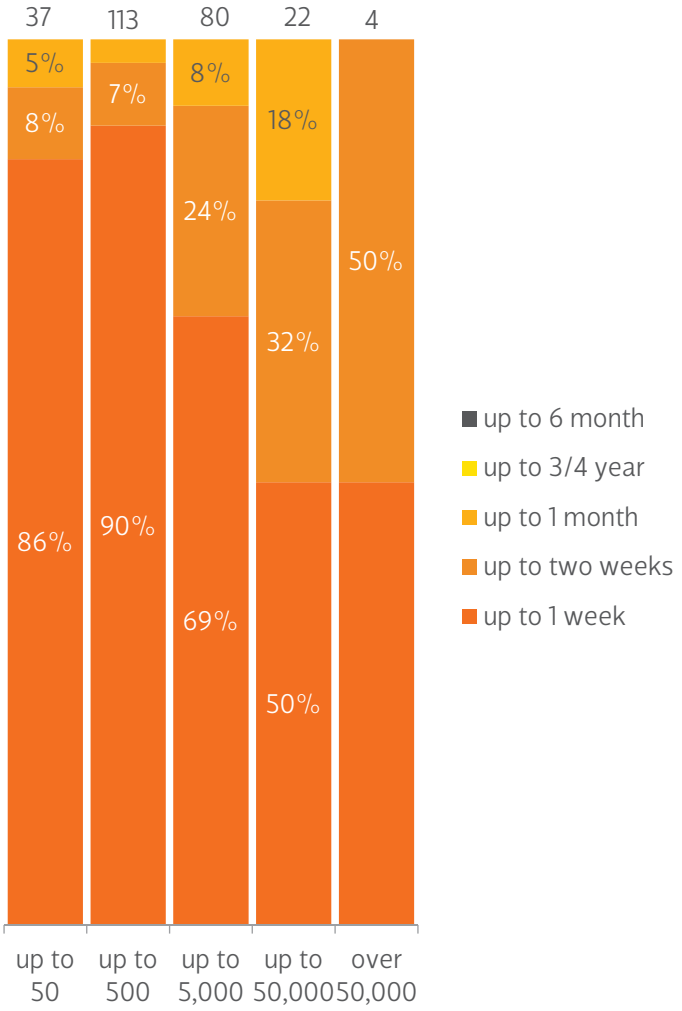
Answers to a question about preferred forms of CPD are sure to be biased by personal experience, but they, nevertheless, reflect the specific needs of the respondents. As was seen in 2012, there is a distinct preference among data protection officers for CPD in the form of external training events. 81% of the respondents stated that they preferred to participate in external training events. Self-study is preferred by 12% of respondents, while online training so far only attracts 5%. This result is unsurprising in the light of the specific need for CPD. In-company data protection practitioners rely on highly specialized CPD that is generally not available either as an online course or in the form of internal training. Self-study is also only useful to a limited extent for imparting highly up-to-date knowledge and competences.

6. How many days have you devoted in the past year to CPD in data protection?

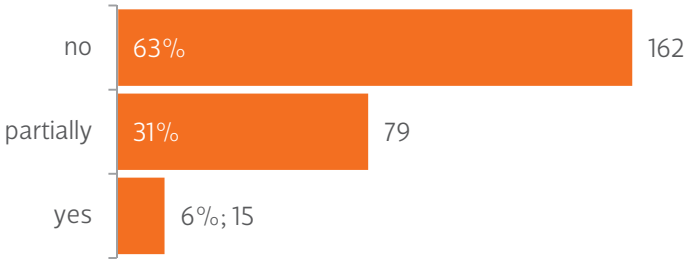


The average response of the data protection officers questioned was five days invested in their own data protection training. If one considers the distribution of CPD activity duration in relation to the size of the company in which the data protection officer works, it can be seen that training events of up to one week in length are common in small and medium-sized companies, while, in larger companies, training events of up to two weeks are more commonly attended.

Here is an overview of the training intensity in correlation to the size of the company:



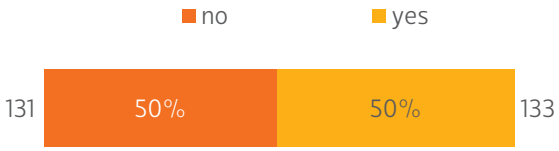
7. Is there an examination at the end of these CPD events?



Only 37% of the CPD events attended by the data protection officers included a full or partial examination of the training outcomes. No examination was held in the other 63% of training activities.

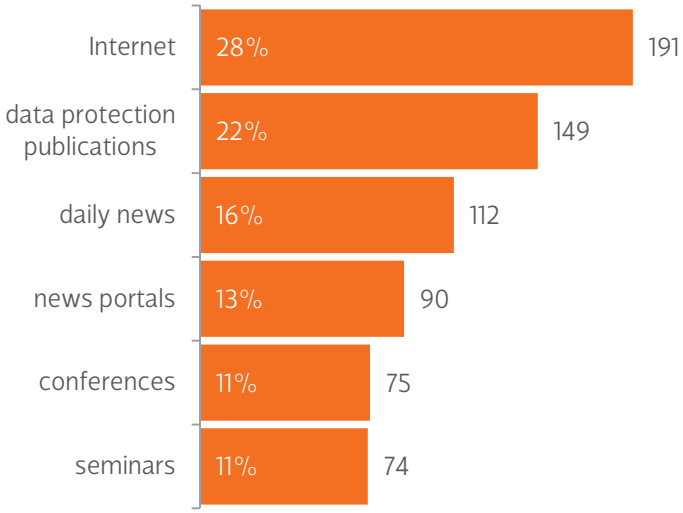
4.10 The New EU Data Protection Regulation

1. Have you read the EU Data Protection Regulation in the version produced after the EU Parliamentary consultation?



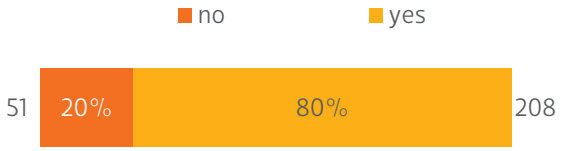
Half (50%) of the data protection officers had read the EU Data Protection Regulation in the version created after the parliamentary consultation by the time of the survey (roughly two months after publication). The level of interest in the first draft was similar in 2012.

2. How have you stayed informed about this regulation up to now?



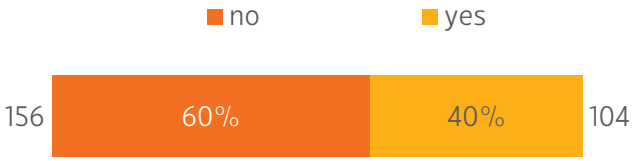
Most of the respondents had relied on the Internet (28%), data protection journals (22%) and the daily newspapers (16%) for ongoing information on the EU Data Protection Regulation. Less frequently, conferences and seminars were mentioned (11% each).

3. In your view, is an EU-wide standardization of data protection via a directly applicable ordinance the right way forward?



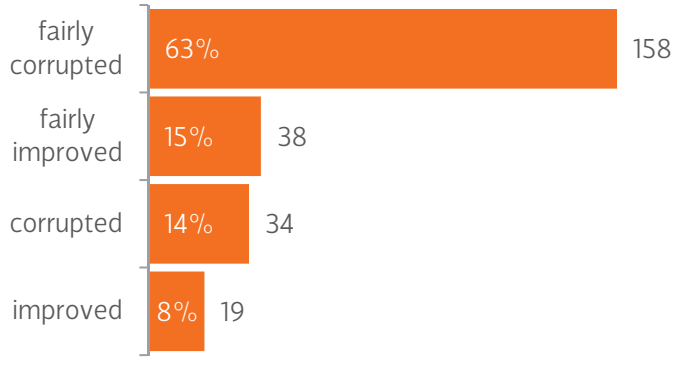
80% of all data protection officers questioned consider standardized data protection throughout the EU to be generally the right way forward. This high value has not changed much since 2012 (81%).

4. Should member states have the right to deviate from the levels of data protection set out in the regulation?



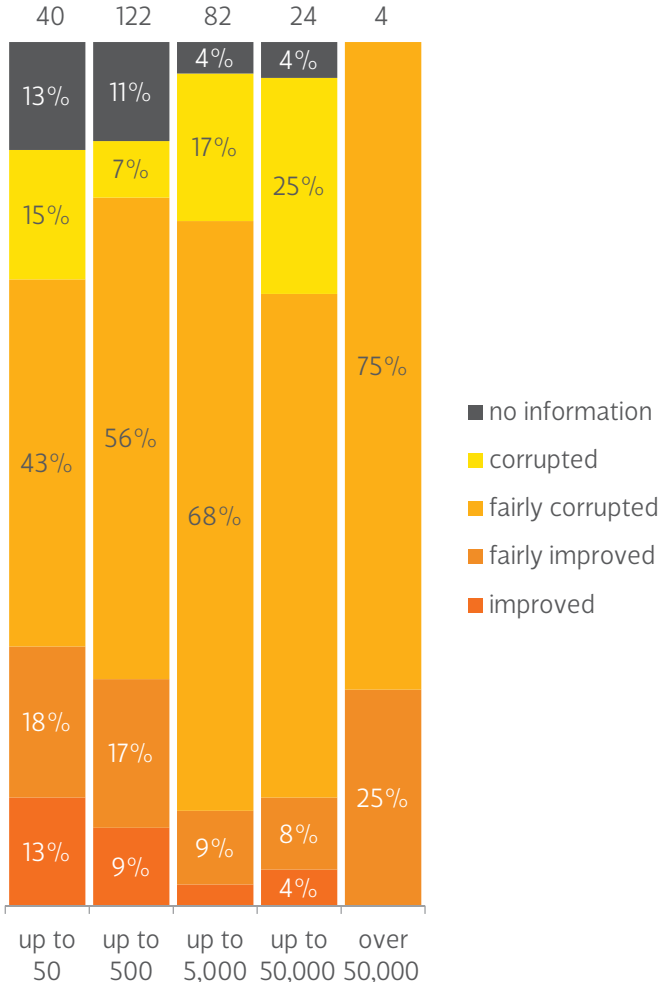
Although a significant majority argue against variations at the national level, 40% of the data protection officers nevertheless would like member states to have the option of deviating from the data protection level set out in the regulation. These views correspond to the survey results for this question in "Data Protection Practice 2012."

5. In your view, would the EU Data Protection Regulation in its current form (after the resolutions of the EU Parliament) tend to improve the level of data protection in Germany or worsen it?

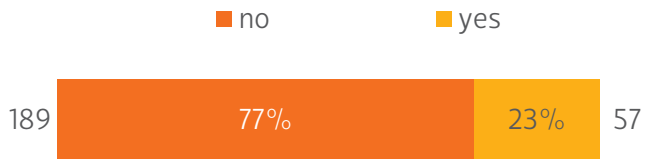


23% of the data protection officers questioned expect an improvement in the level of data protection in Germany, while 77% of those questioned anticipate it to worsen. The level of expectation has dropped significantly here. In 2012, 41% of data protection officers expected an improvement in the level of data protection, while in 2014 the skeptics are even more pronounced.

Here is an overview of the responses to 4.10.5 in relation to company size:

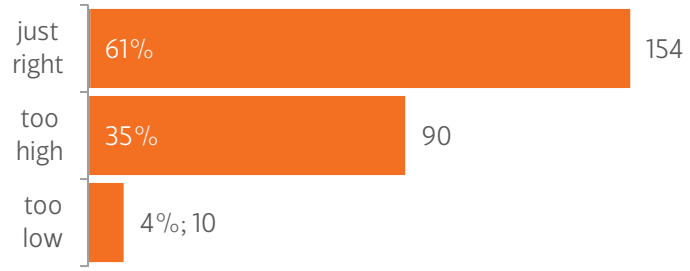


6. In your view, do data subjects have better control over their data under the EU Data Protection Regulation?



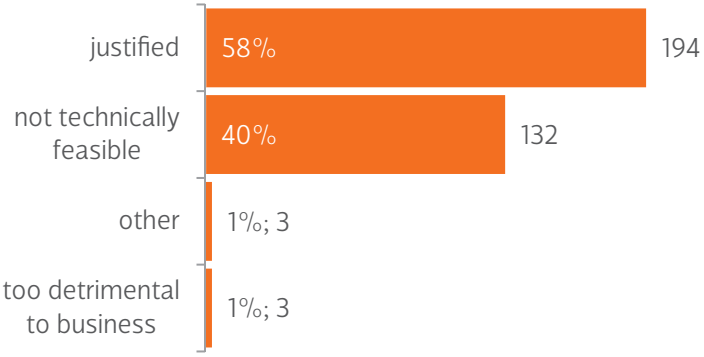
In the German understanding of data protection, the right to informational self-determination is intended to allow data subjects to have control over their data. The Commission is also committed to this objective in its implementation of article 8 of the Charter of Fundamental Rights, article 16 of the Treaty on the Functioning of the European Union and in article 8 of the European Convention on Human Rights. As was already seen in the results of "Data Protection Practice 2012," the data protection practitioners are nevertheless largely doubtful about the feasibility of realizing this objective. 77% do not believe that the data subject will regain control over his or her data as a result of the EU General Data Protection Regulation.

7. What is your view on the amount of the intended fines of €100 million or up to 5% of global turnover?



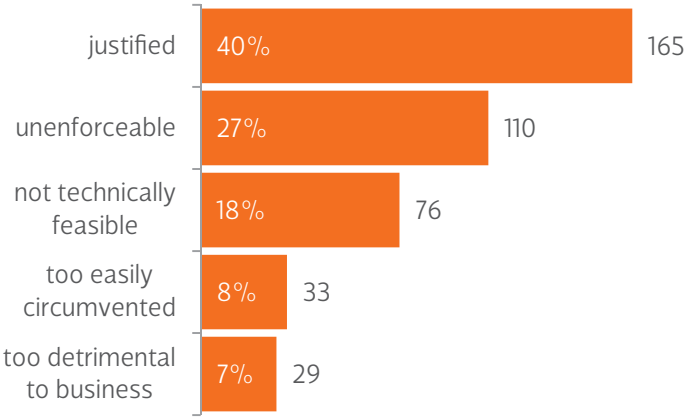
The verdicts of the data protection officers on this penalty framework are relatively evenly balanced. 61% of respondents consider fines of up to €100 million or up to 5% of global turnover as "exactly right," 4% as "too low" and 35% as "too high."

8. How do you view the right to delete personal data on social networks?



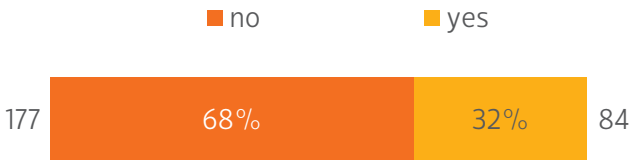
The right to remove personal data in social networks is considered correct by 58% of respondents, though 40% see it as not technically feasible. This shows a clear support of the intention but also doubts as to the technical feasibility of these proposals. This assessment has hardly changed compared to 2012.

9. How do you view the fact that if a company transfers data to another party, it must notify the recipient of any request for deletion it subsequently receives, even after the transfer has taken place?



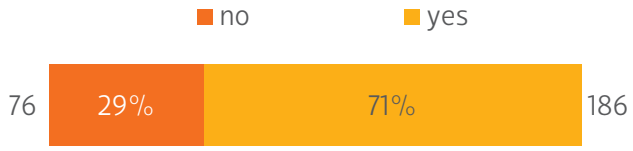
Data transfers are an everyday occurrence in our networked economy and this poses the greatest problem in enforcing a deletion request. The proposed obligation to notify data recipients of an intention to delete ("deletion chain") is considered correct by 40% of the data protection officers, as was also the case in 2012, yet 60% doubt its enforceability (too harmful to enterprise, technically unrealizable, too easily bypassed or combinations of these).

10. Rather than the Commission's proposal for businesses with over 250 employees, a data protection officer should now be appointed if the data of over 5,000 customers is processed within a period of 12 consecutive months. Do you consider it correct that the obligation to appoint a data protection officer should be linked to the number of data sets regularly processed in the company?



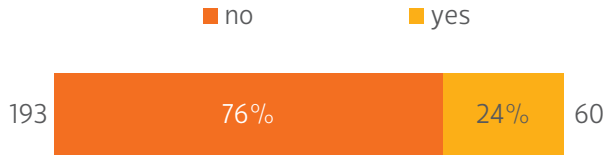
Only 32% of the participating data protection officers consider it correct for the obligation to appoint a data protection officer to be linked to the number of data sets regularly processed in the company; a clear majority of 68% consider this the wrong approach.

11. Do you welcome the registration of data protection officers by name with the regulatory authority?



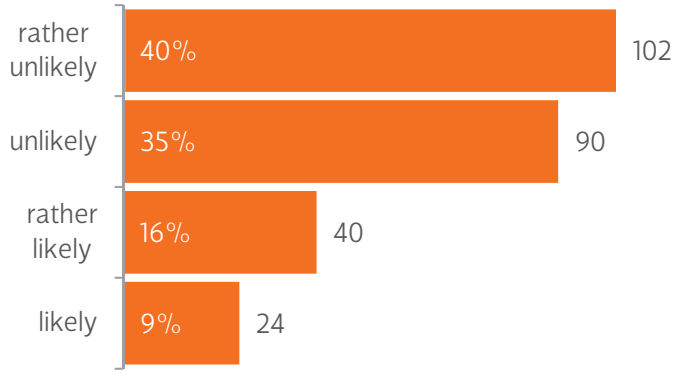
The obligation to register data protection officers by name with the regulatory authority is welcomed by 71% of the respondents. Compared to the results of "Data Protection Practice 2012," in which 57% of data protection officers welcomed this development, a continuing positive trend can be observed.

12. Do you think that the new EU Data Protection Regulation will make your work as a data protection officer easier?



Again in 2014, only 24% of the participating data protection officers anticipate that the new EU General Data Protection Regulation will make their work easier.

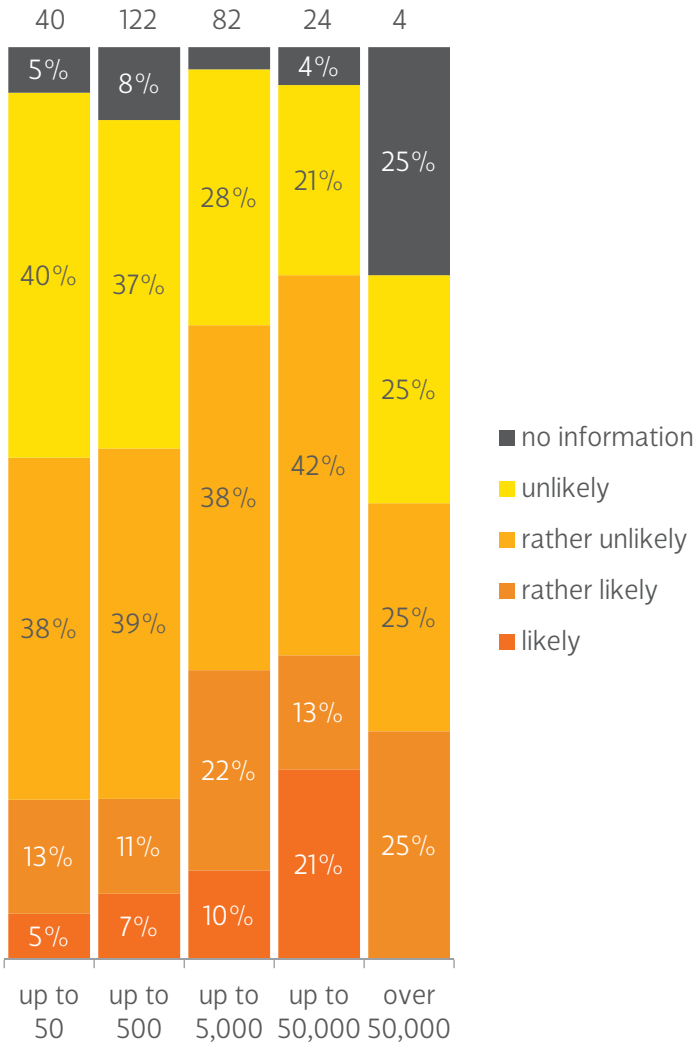
13. The draft EU Data Protection Regulation contains detailed regulations on Binding Corporate Rules (BCR), which are intended to simplify the transfer of personal data to other countries and also within a corporate group. How probable do you think it is that your company will make use of these Binding Corporate Rules (BCR) in the future?



25% of participating data protection officers consider it probable or fairly probable that use will be made of BCR in their company in future. In 2012, 40% still considered this probable or fairly probable. In general, interest in Binding Corporate rules has fallen considerably since the results of "Data Protection Practice 2012" were obtained. This can be seen particularly among the larger companies with more than 5,000 employees.

Article 43 of the draft General Data Protection Regulation makes data transfers on the basis of binding internal corporate rules permissible if a regulatory authority has authorized binding internal corporate rules in accordance with the consistency mechanism described in article 58. Despite the immense expenditure required for such a procedure, in 2012, the practitioners of the large companies in particular considered it probable that their company would make use of this regulation in the future. In 2014, data protection officers from large companies have a greater tendency to view this as unlikely.

Here is an overview of the responses to 4.10.13 in relation to company size:



2B Advice

The Privacy Benchmark

2B Advice GmbH
Joseph-Schumpeter-Allee 25
53227 Bonn
Phone: +49 228 926165-100
Fax:+49 228 926165-109
Email: info@2b-advice.com

www.2b-advice.com